



ExpertNet™ Lite Assessment Tool

User Guide

May 2008

© 2008 Avaya Inc. All rights reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

About this guide

This guide is intended for BusinessPartners and Avaya Associates using the ExpertNet™ Lite Assessment Tool (ELAT) for the first time. It describes how to get started and how to use ELAT for customers purchasing an IP Telephony solution that requires an IP Network Readiness Assessment.

About the ExpertNet™ Lite Assessment Tool

ELAT is a software application designed to gather information from an IP network. The data gathered is used to produce a Network Readiness Assessment report. It is designed to run for an extended period of time (usually 5 days), in order to see trends in network performance. The data is summarized graphically and can be included in the report.

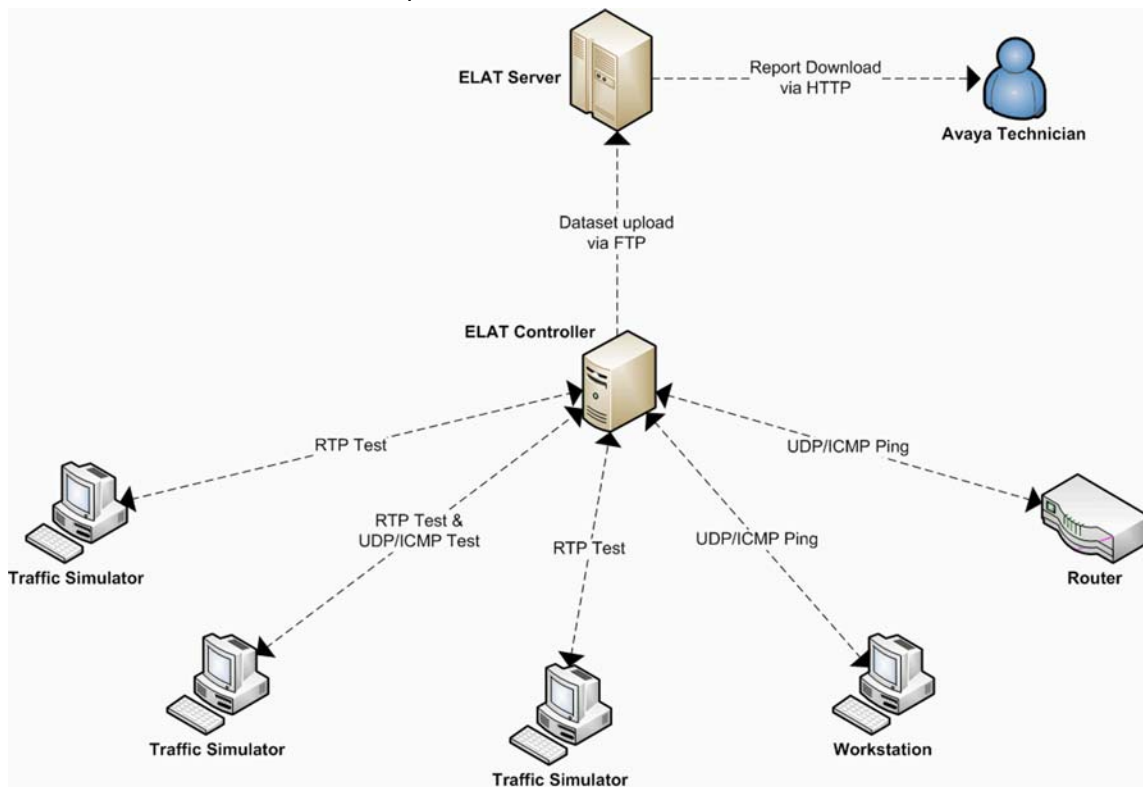
Three types of queries are used to perform the measurements: RTP tests, ping probes and SNMP GET requests.

- ELAT provides RTP test functionality through the use of Traffic Simulators, which are installed on remote machines on the customer network.
- ELAT supports two ping protocols: UDP (default) and ICMP. On some networks, the default UDP protocol may not work. (For example, a firewall may be configured to block traffic to certain ports.) In such cases, the user can switch the protocol to ICMP.
- ELAT Controller supports SNMPv1 and SNMPv2 protocols. It collects processor and layer-3 interface utilization variables from devices on network paths. For the Controller to be able to retrieve SNMP data, it must be configured with a list of SNMP community strings.

The ELAT Controller collects Round Trip Time and One Way Delay measurements along network paths. Network paths can be entered manually by the user, or discovered automatically. To discover paths automatically, the Controller employs, transparently to the user, a bundled ExpertNet Discovery Tool. The EDT tool discovers network topology in a scope configured by the user.

ExpertNet Lite Assessment Tool Architecture

- ExpertNet™ Lite Assessment Tool Controller – Runs on a PC to measure delay and packet loss and to produce a dataset.
- Avaya Traffic Simulator – A remote agent that is deployed on various PCs on the customer network to work with the ELAT controller.
- Dataset from the agent in the form of a compressed file is uploaded automatically or manually to the FTP server.
- ExpertNet™ Lite Assessment Tool Server – Analyzes uploaded datasets to produce graphical representations that can be browsed or included in the Network Assessment Report.



Requirements for ELAT Controller

Hardware

- Standard IBM PC-compatible
- Intel x86 CPU or compatible, Pentium 1Ghz performance
- 512MB of RAM for Windows XP
- 3GB free disk space.

Operating System

- Windows XPTM Professional Edition with Service Pack 2
- .Net framework 2.0 preferable.

Network

- 100Mb /s (or greater) Ethernet adapter (NOTE: If multiple NIC's exist, it is preferable, but not required, to disable all but one)

Requirements for Avaya Traffic Simulator

Hardware

- Standard IBM PC-compatible
- Intel x86 CPU or compatible, Pentium 1Ghz performance
- 512MB of RAM for Windows XP
- 150MB free disk space.

Operating System

- Windows XPTM Professional Edition with Service Pack 2
- .Net framework 2.0

Network

- 100Mb /s (or greater) Ethernet adapter (NOTE: If multiple NIC's exist, it is preferable, but not required, to disable all but one)

Installing ExpertNet Lite Assessment Tool Controller

Before installing ELAT, please ensure that all PCs on which ELAT will be installed are set up as follows:

- Disable screen savers.
- Disable any time synchronization services.
- Check the Power control panel and disable any options that make the PC move from the active state.
- Verify the current time and date.
- If the Controller PC has time synchronization services enabled, there is a potential problem of having the Controller PC time roll back to some past time. To avoid this, disable the time synchronization services during the ELAT run on the Controller PC.
- Disable virus scan and SMS software.

It is preferable, but not essential, that you:

- Disable all background services, like Office Find, Indexing Service, SETI@home, etc.
- If you have multiple NICs installed, enable only one NIC and disable all other NICs.

Obtain the ELAT License File

After purchasing a 30-day ELAT subscription, email the ELAT administrator (elatadmin@avaya.com) to obtain a license file. When you receive the file (license.txt), save it in the ELAT **config** directory (by default it is **C:\Program Files\Avaya\ELAT\config**).

BusinessPartners

After you have purchased a 30-day subscription, you can install ELAT on as many machines as you like at the customer site. Once installed, the license permits 30 days of usage.

Avaya Engineers

You do not need to purchase a subscription, but can generate one from ESDP directly.

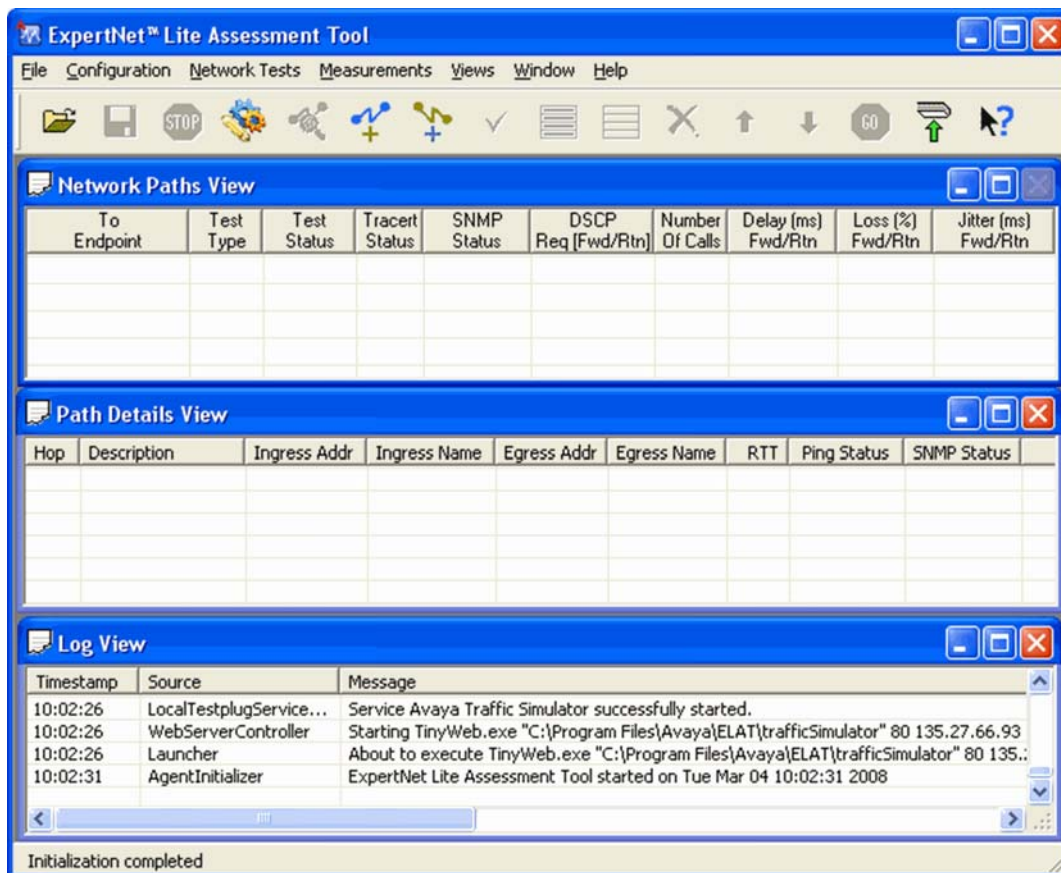
Install the Controller

Download the ELAT Controller (a 40Mb binary file) from <http://support.avaya.com>.

The installation typically takes less than 5 minutes. For more detail about installing the Controller, refer to [Appendix A: Installing the Controller and Test Agents](#).

Launch the Program

After you have installed the ELAT Controller application and copied a valid license file to the **config** directory, you can launch the ELAT Controller. To launch ELAT select: **Start > All Programs > Avaya > ExpertNet™ Lite Assessment Tool > ExpertNet™ Lite Assessment Tool > Controller**. The main window is displayed:



Configuring the ELAT Controller

To run the ELAT Controller Configuration wizard, select **Configuration > Modify Configuration**. You can review all the parameters and accept the defaults or change any parameter as per your network needs. The most frequently modified parameters are:

- **Data Collection Interval** from the General Settings page.
- Community strings from the **Read SNMP Community Strings** page. (Without the SNMP community strings ELAT cannot retrieve CPU and other metrics of devices and the report will not be as detailed.)
- Topology option from the **Network Discovery Options** page.

Other configuration parameters rarely require modification.

Step 1. General Settings

This page allows to set up general settings for the tool. Most fields will not need to be changed.

The screenshot shows the 'ExpertNet™ Lite Assessment Tool - Configuration Wizard' window. The title bar includes a help icon and a close icon. The main window is titled 'Step 1: General Settings'. On the left, there is a vertical navigation pane with four icons representing different configuration steps. The main area contains the following settings:

- Data Collection Interval:** 5 (text input) and day (dropdown menu)
- Logging Verbosity Level:** high (dropdown menu)
- Web Server Port:** 80 (text input)
- FTP User Name:** expertnetlite (text input)
- FTP Password:** masked with asterisks (text input)
- FTP Server:** ftp.avaya.com (text input)

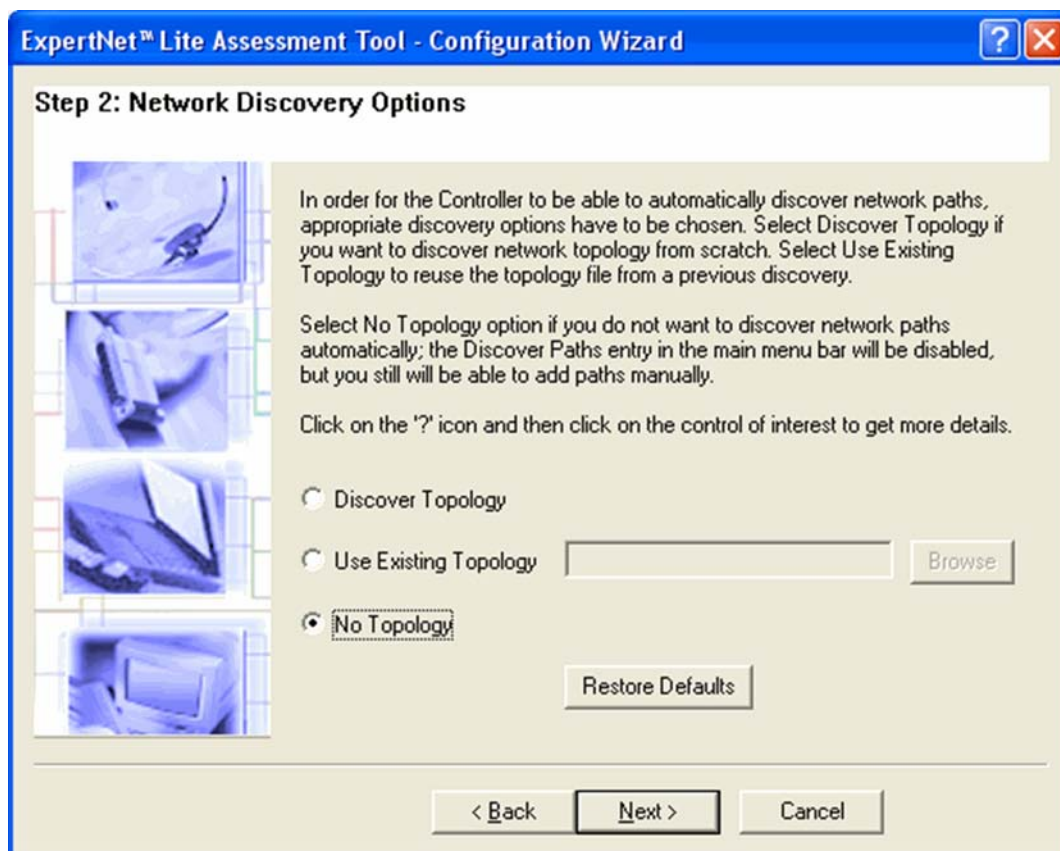
Below the settings is a 'Restore Defaults' button. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

| | |
|---------------------------------|---|
| Data Collection Interval | Specify the period for which the ELAT Controller will collect data. At the end of this period, ELAT will stop running tests and automatically upload the data to the Avaya FTP Server. The default interval is 5 days. |
| Logging Verbosity Level | Select the level of detail the logging subsystem will store in the log file. You can select: None, Low, Medium, and High. The default is High. |
| Web Server Port | Enter the port number of the bundled Web Server for downloading the RTP Traffic Simulator to remote endpoints. To download the Traffic Simulator, point the Web browser to http://<controller_IP_address>:<port_number> |
| FTP User Name* | Enter the user name of the FTP Server account for uploading data to Avaya. |
| FTP Password* | Enter the password of the FTP server account for loading data to Avaya. |
| FTP Server* | Enter the name of the FTP Server to which the data is uploaded. |

* Default values for these fields should never be changed.

Step 2: Network Discovery Options

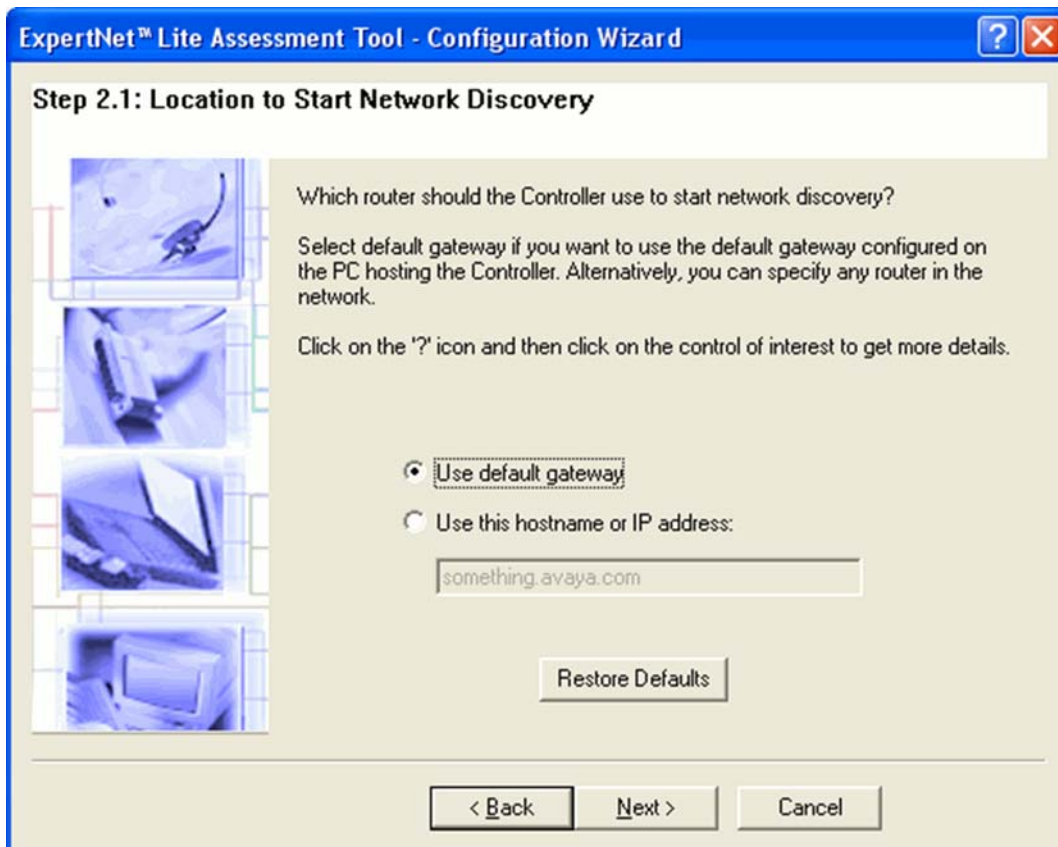
Each time the user selects **Network Paths > Discover Paths** menu item from ELAT's main menu, the EDT tool discovers the network and leaves behind a topology file. (The default location is **C:\Documents and Settings\\My Documents\Avaya\ExpertNet Discovery Tool\topology_files\ topology.vpa**). This file can be reused next time the user wants to discover paths.



| | |
|------------------------------|---|
| Discover Topology | Select this option if you want the Controller to discover network topology from scratch. Steps 2.1 and 2.2 in the Configuration Wizard are enabled. You must have SNMP access to network routers to use this option. |
| Use Existing Topology | Select this option if you want the Controller to reuse the existing topology file from a previous discovery. |
| No Topology | Select this option if you do not want to (or cannot) discover network paths. The Network Tests > Discover Ping Tests entry in the main menu bar will be disabled, but you will still be able to add Ping tests manually. You may want to consider this option if SNMP access to network routers is not allowed. |

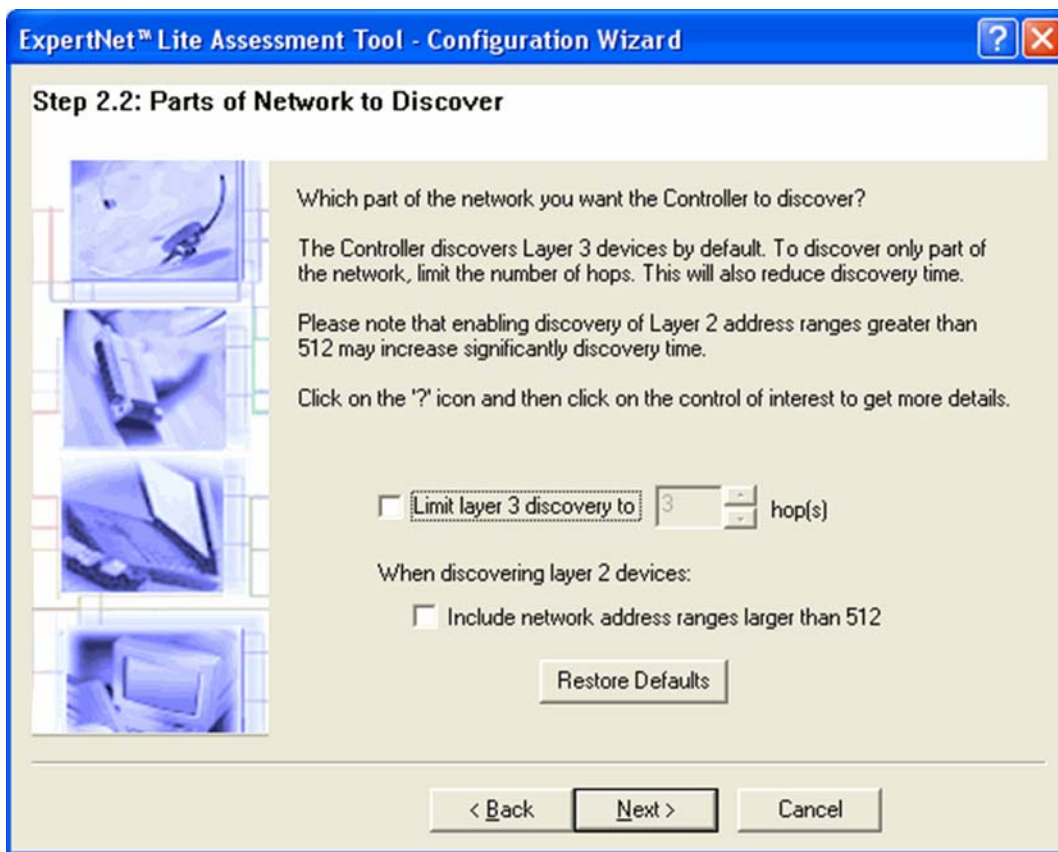
Step 2.1: Location to Start Network Discovery

Steps 2.1 and 2.2 will only display if you selected the Discover Topology option.



| | |
|--|---|
| Use default gateway | Select this option if you want the Controller to use the default gateway configured on the Controller PC to start network discovery from. |
| Use this hostname or IP address | Select this option if you want the Controller to use a specified initial gateway to start network discovery from. |

Step 2.2: Parts of Network to Discover



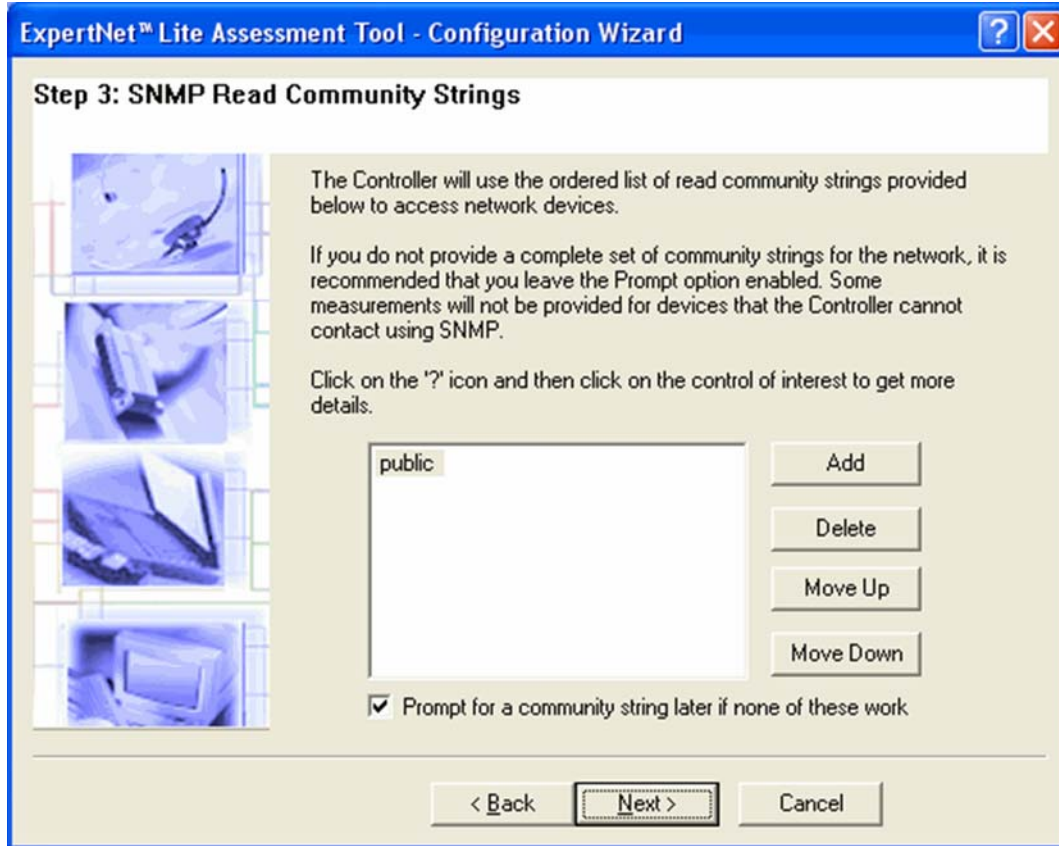
| | |
|---|--|
| Limit layer 3 discovery to <n> hops | Select this option if you want to limit the scope of network discovery to a specified number of hops (routers) on network paths. |
| Include network address ranges larger than 512 | Select this option if you want to scan ranges of network addresses greater than 512 in search of layer 2 devices. Discovery time may increase significantly if you select this option. |

Step 3: SNMP Read Community Strings

Read Community strings are used to retrieve SNMP data from the customer network. Without the community strings we cannot retrieve performance criteria (CPU, interface) from devices.

If your customer does not want to give you the community strings, a workaround is to ask the customer to create temporary Read community strings that expire or will be deleted when ELAT has concluded data collection. Once the community strings expire or are deleted, the community strings in the dataset will no longer be valid and will not compromise the customer's network. We recommend "public" or "Avaya" as the Read community strings. Please have the customer verify that the community strings will expire after data collection has concluded.

If the customer is not willing to allow this level of access you can proceed without read community strings. Performance criteria data will not be collected.



Add the appropriate SNMP read community strings, and prioritize using **Move Up** and **Move Down** buttons. Select the **Prompt for a community string later if none of these work** option if you want a warning to display when a device is discovered that does not use any of the configured strings.

Deselect this option if the customer has not given you the read community strings.

Step 4: SNMP Settings

On this page you can set values for SNMP requests sent on the network. These settings rarely need to be changed.

ExpertNet™ Lite Assessment Tool - Configuration Wizard

Step 4: SNMP Settings

This page allows you to set values for SNMP requests sent on your network to obtain network performance data, such as router interface utilization and CPU usage. These settings rarely require modification.

Click on the '?' icon and then click on the control of interest to get more details.

Poll Interval of Single Node [secs]

Maximum Total Number of Polls/Sec

Number of Request Retries

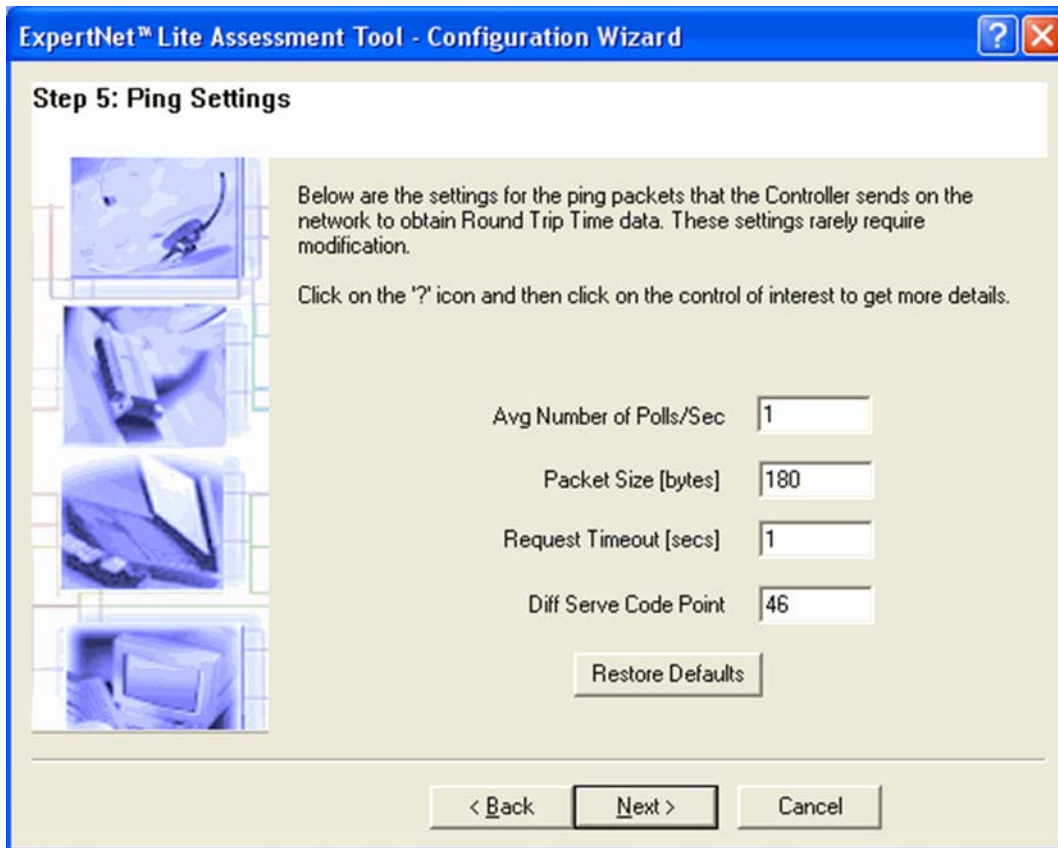
Request Timeout [secs]

< Back Next > Cancel

| | |
|--|--|
| Poll Interval of Single Node | Poll interval defines the interval for sending SNMP requests to a single node on the network. The default Poll Interval is 120 seconds. |
| Maximum Total Number of Polls/Sec | Used to set network throttling by limiting the number of SNMP requests per second sent to all nodes. This setting takes precedence over Poll Interval: if Poll Interval is too small, it is automatically recalculated by the Controller to satisfy the Maximum Total). Default setting is 2 polls per second. |
| Number of Request Retries | Defines the number of times the SNMP request is sent to a network device if the response does not arrive within the period set in the Request Timeout field. The default setting is 1. |
| Request Timeout (secs) | Defines how many seconds the Controller will wait for a response to an SNMP request before sending a retry. The default setting is 5 seconds. |

Step 5: Ping Settings

On this page you have the option to change the default settings for Ping tests run on the network. Again, these settings rarely need to be modified.



| | |
|------------------------------------|--|
| Average Number of Polls/Sec | Determines the frequency of sending ping probes to the network. The default setting is 1 ping per second. |
| Packet Size (bytes) | Used to set the size of the packets sent by the Controller. The value is in the byte size of the ping packet, without IP and Ethernet headers. The default setting is 180 bytes. |
| Request Timeout (secs) | Defines how many seconds the ELAT Controller will wait for a response to a ping before it qualifies the packet as lost. The default setting is 1 second. |
| Diff Serv Code Point | Defines the Differentiated Services Code Point of the IP Packet. By default this value is 46 (Expedited Forwarding). |

Step 6: RTP General Configuration

On this page you have the option to change the default settings for RTP tests run on the network. All RTP tests that are added automatically will use these settings. You can manually add further RTP tests with different settings when the Wizard settings are configured.

ExpertNet™ Lite Assessment Tool - Configuration Wizard

Step 6: RTP Test Settings

Below are the settings for RTP Tests. Click on the '?' icon and then click on the control of interest to get more details.

Codec: g.729

Diff Serv Code Point: 46

Voice Payload Size [ms]: 20

Number of Simultaneous Calls: 2

Test Duration [sec]: 30

Automatically Create RTP Tests

SNMP Polling

Traceroute

Discover Paths Protocol: UDP

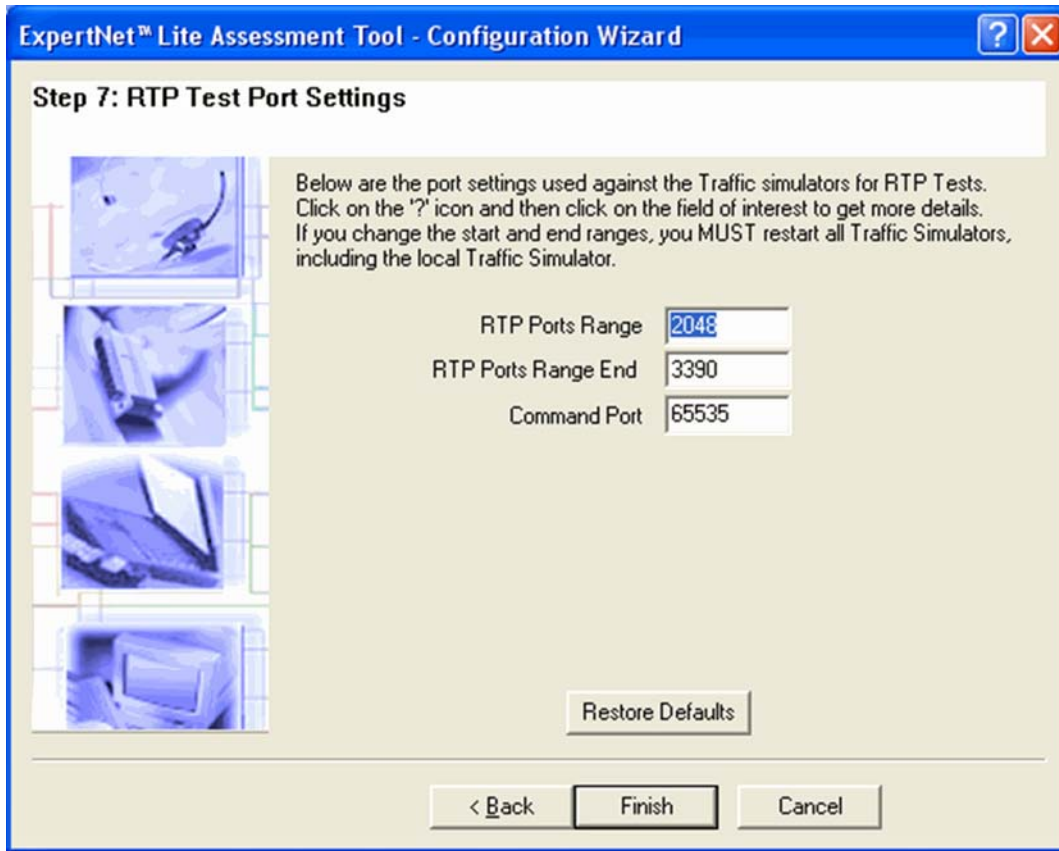
Restore Defaults

< Back Next > Cancel

| | |
|---------------------------------------|--|
| Codec | Defines the Codec of the RTP test calls. This will alter the rate and size of packets being sent between Traffic Simulators in order to emulate the G.711 and G.729 codecs. |
| Diff Serv Code Point | Defines the Differentiated Services Code Point (DSCP) of the IP Packets of RTP test calls. Routers will treat packets differently depending on the DSCP value set in outgoing packets. By default this value is 46 (Expedited Forwarding). |
| Voice Payload Size (ms) | Defines the Voice Payload size of the RTP packets of a test call (in milliseconds). Must be a multiple of 10. |
| Number of Simultaneous Calls | Defines the number of RTP test calls to execute simultaneously for a single test. The default value for this setting is 2. Measurements for each call can only be taken in one direction. When two or more calls are configured, half of them originate at the Controller and half at the test agent so data is collected in both directions providing a more complete assessment of the network than if a single call were run. |
| Test Duration | Defines the duration of each RTP test call (in seconds). |
| Automatically Create RTP Tests | Check this box to allow the Controller to automatically create new RTP test Calls from the Controller to the RTP Traffic Simulator as the simulators register. |
| SNMP Polling | Check this box to allow the Controller to enable SNMP polling for RTP test calls. |
| Discover Paths | Check this box to allow the Controller to use traceroute to discover the paths between the Controller and the Traffic Simulators during RTP test calls. |
| Protocol | Select a traceroute protocol to be used to discover routers on the test path. The default setting is UDP. |

Step 7: RTP Ports Configuration

In this page you must configure the port settings that will be used against the test agents.



| | |
|----------------------------|---|
| RTP Ports Range | Defines the starting port for the range of ports which can be used for RTP tests. The typical range for RTP tests used by Avaya is 2048 to 3390, but any other range between 1024 and 65535 can be used. The range needs at most 100 unobstructed ports to operate correctly. |
| RTP Ports Range End | Defines the ending port in the range used for RTP tests. |
| Command Port | Defines the port used by the Avaya Traffic Simulator to receive commands. The default is port 50000. If this is changed, the same change must be made in the Local Command Port field in the Remote Traffic Simulators |

Install and Configure the Avaya Traffic Simulator

Installing the Avaya traffic Simulator

Install the Avaya Traffic Simulator on each remote endpoint you want to test. Each remote endpoint **MUST** be on the same Voice VLAN on which the VoIP equipment will be eventually installed. Each Traffic Simulator will take approximately 2 minutes to install.

See [Appendix A: Installing the Controller and Test Agents](#) for information on installing the test agents.

Configuring the Avaya Traffic Simulator

When you restart the PC after installing the Traffic Simulator, the application icon will display in your taskbar. The icon displays in red if the tool is not running and in green if it is. Configure the test agent using the following process:

1. Double-click the icon in the task bar.
2. Ensure the IP address in the **ExpertNet Controller** field is the IP address of the PC with the controller installed.
3. In the **Local Command Port** field, enter the port number that will be used to receive commands. This value should match the **Command Port** value in step 7 of the ELAT Configuration Wizard and should not be changed unless required by the network or firewall configuration.
4. Adjust the log level as appropriate for your needs. Setting this value to max may have an adverse effect on the accuracy of results. Setting it to max would only be required whenever there is a problem that requires debugging by support engineers for ELAT.
5. Click **OK**.

When the test agents are configured they should automatically register with the Controller. An RTP test will be automatically created for each end-point. These will display in the network Paths View. This will be explained in detail in the next section.

Adding RTP Tests and Ping Tests - Populating the Network Paths View

Add RTP Tests

About RTP Paths

An **RTP path** is a route from the ELAT controller to an edge PC that has the Avaya Traffic Simulator installed. RTP paths can optionally be tracerouted. As metrics are collected for RTP paths, they will be displayed in the Delay, Jitter and Loss columns.

If RTP paths are tracerouted, the routers discovered are represented in the Path Details View for any selected path. By contrast, an **RTP path without traceroute** is a route from the Controller to a target device through a "cloud" of unknown network nodes.


Adding RTP Tests Automatically

RTP tests can be created for endpoints that have the Traffic Simulator installed, running, and configured. RTP tests will automatically be created for these endpoints as they register if the **Automatically Create RTP Tests** option is selected in **Step 6** of the Wizard. These RTP tests will use the default settings configured in the Wizard.

Adding RTP Tests Manually

If the **Automatically Create RTP Tests** option is not selected, or if you want to add multiple RTP tests with different parameters to the same endpoint, you can use the Add RTP Tests option to manually add tests.

Creating multiple tests to the same endpoint can be useful for determining if varying the values can yield different results. For example adding a test to the same endpoint and then changing the codec or the DSCP value could improve the RTP test results.

To add a new RTP test, select **Add RTP Test** item from the **Network Paths** menu or click the toolbar icon .

Please follow on-screen instructions and context-sensitive help available in the **Add RTP Test** dialog.

Add RTP Test ? X

This dialog enables the user to add a RTP test to a registered Traffic Simulator on the network. Click on the '?' icon and then on the control of interest to get more details.

To Endpoint:

Codec:

Diff Serv Code Point:

Voice Payload Size: ms

Number of Simultaneous Calls:

Test Duration: sec

Traceroute

Discover Path Protocol:

SNMP Polling

To ProtocolSelect a traceroute protocol to be used to discover intermediate routers on

| | |
|-------------------------------------|---|
| To Endpoint | Select an endpoint to which the RTP test is to be created. If Traffic Simulators are connected and registered with the Controller, they will be available in the drop-down menu for use in making new RTP tests |
| Codec | Defines the Codec of the RTP test calls. This will alter the rate and size of packets being sent between Traffic Simulators in order to emulate the G.711 and G.729 codecs. |
| Diff Serv Code Point | Defines the Differentiated Services Code Point (DSCP) of the IP Packets of RTP test calls. Routers will treat packets differently depending on the DSCP value set in outgoing packets. By default this value is 46 (Expedited Forwarding). |
| Voice Payload Size | Defines the Voice Payload size of the RTP packets of a test call (in milliseconds). Must be a multiple of 10. |
| Number of Simultaneous Calls | Number of equivalent VoIP calls for a selected codec in a single test. The default value for this setting is 2. Measurements for each call can only be taken in one direction. When two or more calls are configured, half of them originate at the Controller and half at the test agent so data is collected in both directions providing a more complete assessment of the network than if a single call were run. |
| Test Duration | Defines the duration of each RTP test call (in seconds). |
| Discover Path | Check this button if you want the Controller to discover intermediate routers on the path to the endpoint. |
| Protocol | Select a traceroute protocol to be used to discover intermediate routers on the path to the selected endpoint. |
| SNMP Polling | Check this button if you want the Controller to collect SNMP statistics for devices on this path. |

Add Ping Tests

About Ping Paths

A **ping path** is a route from the ELAT controller to any edge device. Ping paths may optionally be tracerouted.

Like RTP paths, if Ping paths are tracerouted, the routers discovered are represented in the Path Details View for any selected path. In this display it will show their ingress and egress interfaces along with other information. The last IP address on the path always belongs to a Layer 2 edge device. By contrast, a **ping path without traceroute** is a route from the Controller to a target device through a "cloud" of unknown network nodes.

Adding Ping Tests Automatically


If routers on your network are SNMP-enabled and you know their read community strings, the best option is to let the ELAT Controller discover network paths automatically. To do so, select **Discover Ping Tests** from the **Network Tests** menu

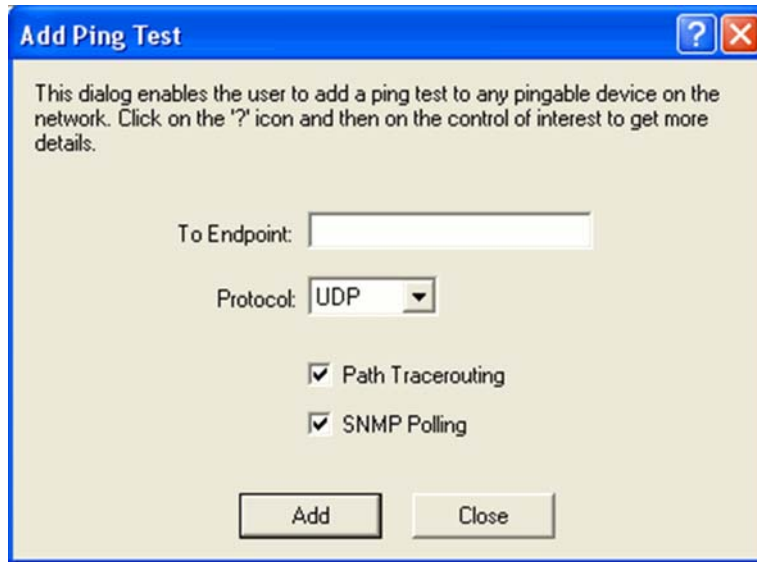
or click the toolbar icon .

The Controller discovers all subnets within a range defined in **Parts of Network to Discover** page of the Configuration Wizard. An initial Ping is sent from the Controller to all end-points in those subnets. When you complete and close the wizard, select **Network Tests > Discover Ping Tests** to automatically add Ping tests in the Network Paths View for all of the endpoints that respond to the initial Ping.

Adding Ping Tests Manually

If you cannot discover paths automatically, or you want to add paths leading to subnets that could not be discovered, select **Add Ping Test** item from the **Network**

Paths menu or click the toolbar icon .



| | |
|--------------------------|--|
| To Endpoint | Host name or IP address of a device that you want to be an edge device of the new ping test path. |
| Protocol | Select a protocol to discover and ping this path. UDP is the recommended protocol. |
| Path Tracerouting | <p>Check this box if you want to use traceroute to discover and ping this path. If the button is not checked, only the edge device will be pinged.</p> <p>With Traceroute: The Controller collects Round Trip Time (RTT) data from ping paths by trace-routing every path periodically. This information is displayed in the Path Details View. The SNMP statistics are collected only for ingress and egress interfaces of every router.</p> <p>Without Traceroute: The Controller collects RTT data from ping paths with traceroute by pinging every target directly. The SNMP statistics are collected for all Layer 3 interfaces of the target device.</p> |
| SNMP Polling | Check this box if you want the ELAT Controller to collect SNMP statistics (CPU and interface utilization) for devices on the test path. |

Understanding the Network Paths View

The screenshot shows two windows from the ExpertNet Lite Assessment Tool. The top window, titled "Network Paths View", displays a table of test results. The bottom window, titled "Details of UDP Ping test from 135.27.66.93 to 10.3.0.20", shows a hop-by-hop traceroute.

| To Endpoint | Test Type | Test Status | Tracert Status | SNMP Status | DSCP Req [Fwd/Rtn] | Number Of Calls | Delay (ms) Fwd/Rtn | Loss (%) Fwd/Rtn | Jitter (ms) Fwd/Rtn |
|---------------|-----------|-------------|----------------|-------------|--------------------|-----------------|--------------------|------------------|---------------------|
| 10.3.0.20 | UDP | OK | ON | Not Cont... | 46/Unknown | | | | |
| 10.5.0.10 | UDP | OK | ON | OK | 46/Unknown | | | | |
| 135.27.67.125 | g.729 | OK | OFF | Not Cont... | 46 | 2 | 0/0 | 0/0 | 0/0 |
| 135.27.67.125 | g.729 | OK | OFF | Not Cont... | 46 | 2 | 0/0 | 0/0 | 0/0 |

| Hop | Description | Ingress Addr | Ingress Name | Egress Addr | Egress Name | RTT | Ping Status | SNMP Status |
|-----|-----------------------|--------------|--------------|-------------|-------------|-----|--------------|--------------|
| 5 | | 32.29.39... | | | | | OK | Not Conta... |
| 6 | | 32.29.23.82 | | | | | OK | Not Conta... |
| 7 | | 135.56.81... | | | | | OK | Not Conta... |
| 8 | | 198.152.2... | | | | | OK | Not Conta... |
| | --- cloud --- reas... | | | | | | | |
| N | | 10.3.0.20 | | | | | Not Pingable | Not Conta... |

All of the Network Paths or Tests that you have created are added in the Network Paths view. The icon at the beginning of each row indicates the type of test. The icons display in red for failed tests. The remaining columns contain further information about the test parameters and results.

RTP Tests

The below image displays the Network Paths view of an RTP test. All of the columns contain data when the test is added. When a test is verified or run the results will be entered in the last three columns, Delay, Loss and Jitter. The test Status may change depending on the test results. The table below explains all of the columns in detail.

The screenshot shows the "Network Paths View" window with two rows of RTP test results. The test status is "OK" for both, and the delay, loss, and jitter are all 0/0.

| To Endpoint | Test Type | Test Status | Tracert Status | SNMP Status | DSCP Reqstd/Recvd | Number Of Calls | Delay (ms) Fwd/Rtn | Loss (%) Fwd/Rtn | Jitter (ms) Fwd/Rtn |
|---------------|-----------|-------------|----------------|-------------|-------------------|-----------------|--------------------|------------------|---------------------|
| 135.27.67.125 | g.729 | OK | OFF | Not Cont... | 46 | 2 | 0/0 | 0/0 | 0/0 |
| 135.27.67.125 | g.729 | OK | OFF | Not Cont... | 46 | 2 | 0/0 | 0/0 | 0/0 |

Tests are run from the Controller to the Traffic Simulator, and from the Traffic Simulator to the Controller. Results are displayed in forward/backward notation. For example, 30/150 indicates that there was 30ms delay forward and 150ms backwards, indicating an asymmetrical network path.

ELAT will traceroute ONLY in the forward direction and not the reverse.

RTP tests offer more complex settings than ping tests and it may be worthwhile having multiple tests to the same endpoint with different settings to see whether there is an impact on the metrics gathered. See "Troubleshooting" on page 35 for more information about RTP tests.

Ping Tests

The following is an example displays two **ping tests** with different settings. As you can see only the first 6 columns contain data. QoS data can only be gathered using RTP tests.

| To Endpoint | Test Type | Test Status | Tracert Status | SNMP Status | DSCP Req [Fwd/Rtn] | Number Of Calls | Delay (ms) Fwd/Rtn | Loss (%) Fwd/Rtn | Jitter (ms) Fwd/Rtn |
|-------------|-----------|-------------|----------------|-------------|--------------------|-----------------|--------------------|------------------|---------------------|
| 10.5.0.10 | UDP | OK | ON | OK | 46/Unknown | | | | |
| 10.3.0.20 | UDP | OK | ON | Not Cont... | 46/Unknown | | | | |

Columns in the Network Path View

The columns in the Network Path View window are as follows:


| | |
|-----------------------|---|
| To Endpoint | The endpoint the test is against, typically an edge PC. The icon indicates the type of test. The phone icon represents an RTP test and the computer icon represents a ping test. |
| Test Type | Shows more precisely the type of tests. For RTP tests, this can say G.711 or G.729, representing the different codecs. For ping tests, this will be ICMP or UDP. |
| Test Status | Indicates the last known state of a test. RTP tests can go into the OK, Failed and Timeout categories. <ul style="list-style-type: none"> - OK - The endpoint responded successfully. - Not Pingable - The endpoint is not pingable. - Timeout - A ping request was sent, but a response was not received. - Off Path - A ping response was received from a device not located on the tracerouted path. - Failed - No results returned for the RTP test |
| Tracert Status | Indicates whether traceroute is enabled or disabled for a path. Will be automatically off if the test is in the same subnet. |
| SNMP Status | Displays whether there is a router/switch in the path which can be contacted using SNMP. <ul style="list-style-type: none"> - OK - SNMP status was successfully obtained. - Not Contactable - The device cannot be contacted. - Not Supported - The device does not support SNMP queries, or the SNMP Polling option has been deselected.. - Timeout - The device did not respond to an SNMP query in time. |


| | |
|--|--|
| DSCP (Differentiated Services Code Point) | <p>This column is useful for determining DSCP problems on the network. The DSCP is shown in a slash notation. The first value is the user-requested DSCP that will be injected into the network with the Ping/RTP packets. The second values show all the DSCP values that were found in the network in a comma separated format. For example:</p> <p>46 46,20/30,0 - means 46 was the priority code of packets sent into the network. On the forward link, packets were received with the setting 46 and 20, and on the backward link, it found packets with the setting 30 and 0. This indicates that the network isn't preserving the DSCP value.</p> |
| Number of calls | <p>Indicates the number of calls that will be run simultaneously on that link. Can run up to 10 calls on a single network link at the same time.</p> |
| Delay/Loss/Jitter | <p>Each column indicates the QoS metric for that column. These will only be populated for RTP tests when a result is obtained, which is at the end of the call length that is configured for that test.</p> <p>These columns will be blank for ping tests.</p> <p>The Traffic Simulator will occasionally fail computing a test and this is represented in the controller as 100% loss and the status <i>Failure</i>. This does not mean your network actually has 100% loss on that link and this can be easily confirmed with a ping test. These results are thrown away for the purposes of graphing so it will not affect the reports.</p> |

When ELAT completes the data collection, it will upload the dataset automatically to the FTP server as configured in the Configuration Wizard.

Verify the Tests

When all of the tests you want to run are configured you should verify them to ensure that they can be run successfully. It is especially important to verify all RTP tests at least once as you may have firewall and port related issues when the tests are started. Any failures should be investigated before commencing the week long measurements. [Appendix B: Firewall Configuration](#) for information on configuring firewalls)


Click the toolbar icon  , or right-click and select **Verify** to verify all selected the tests.

Use the **Select all**  button on the toolbar to select all of the configured tests. Alternatively, use **Ctrl+click** and **Shift+click** to select multiple tests.

Begin Data Collection

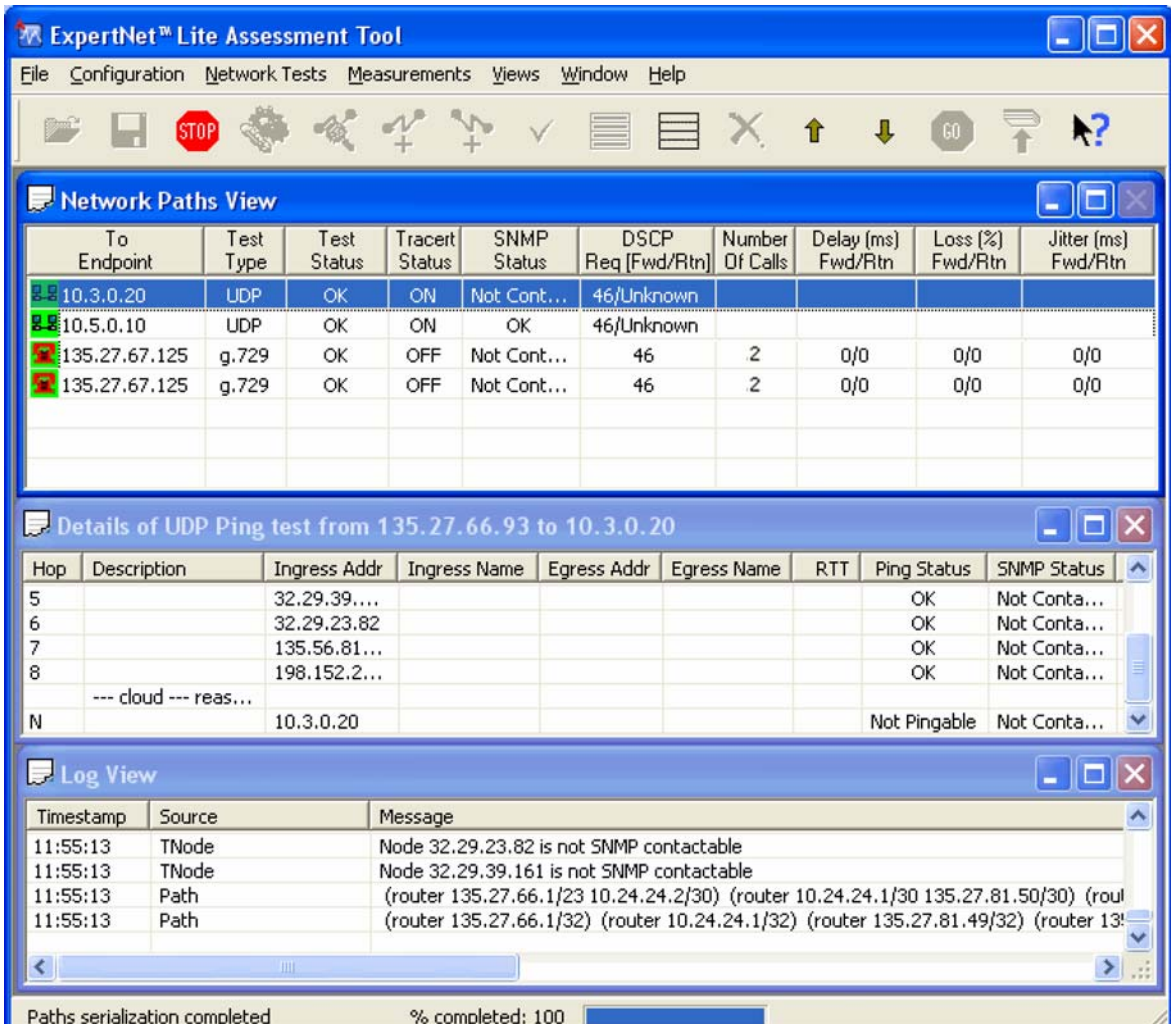
At this point the Network Paths View should be populated with tests that provide a good coverage of your network, and all of these tests should be verified.

Every ping test will collect raw Round Trip Time (RTT) data for all ingress interfaces on the path. Every RTP test will cause a flow of RTP packets through the network and collect QoS data. In addition, each SNMP-contactable router will be polled to collect CPU and interface utilization.

To start collecting RTP, Ping and SNMP measurements, select **Start Measurements** item from the **Measurements** menu or click the toolbar icon .

Data is collected for the **Data Collection Interval** time set in the **General Settings** page of the Configuration Wizard or until stopped.

Leave ELAT running until the test period is over. A progress bar displays at the bottom of the window.



The screenshot displays the ExpertNet Lite Assessment Tool interface. The main window is titled "ExpertNet™ Lite Assessment Tool" and contains several panes:

- Network Paths View:** A table showing test results for various endpoints.
- Details of UDP Ping test from 135.27.66.93 to 10.3.0.20:** A table showing hop-by-hop details for a specific test.
- Log View:** A log of messages from the tool.

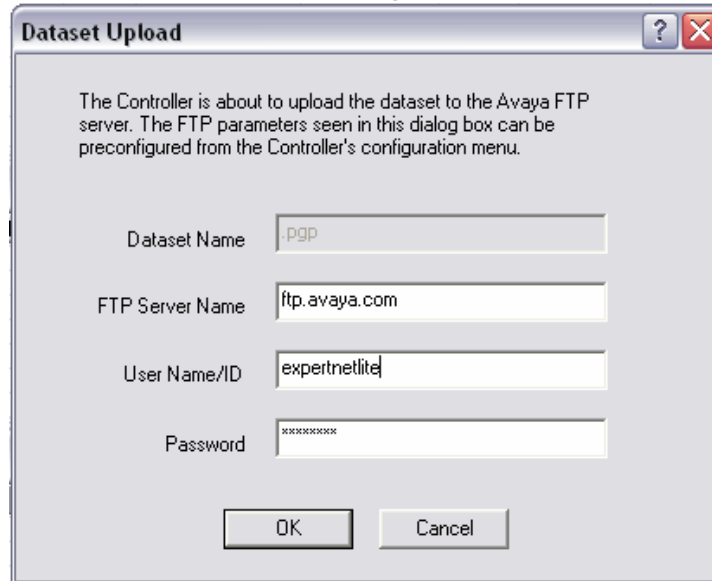
At the bottom of the window, a status bar indicates "Paths serialization completed" and a progress bar shows "% completed: 100".

| To Endpoint | Test Type | Test Status | Tracert Status | SNMP Status | DSCP Req [Fwd/Rtn] | Number Of Calls | Delay [ms] Fwd/Rtn | Loss [%] Fwd/Rtn | Jitter [ms] Fwd/Rtn |
|---------------|-----------|-------------|----------------|-------------|--------------------|-----------------|--------------------|------------------|---------------------|
| 10.3.0.20 | UDP | OK | ON | Not Cont... | 46/Unknown | | | | |
| 10.5.0.10 | UDP | OK | ON | OK | 46/Unknown | | | | |
| 135.27.67.125 | g.729 | OK | OFF | Not Cont... | 46 | 2 | 0/0 | 0/0 | 0/0 |
| 135.27.67.125 | g.729 | OK | OFF | Not Cont... | 46 | 2 | 0/0 | 0/0 | 0/0 |

| Hop | Description | Ingress Addr | Ingress Name | Egress Addr | Egress Name | RTT | Ping Status | SNMP Status |
|-----|-----------------------|--------------|--------------|-------------|-------------|-----|--------------|--------------|
| 5 | | 32.29.39... | | | | | OK | Not Conta... |
| 6 | | 32.29.23.82 | | | | | OK | Not Conta... |
| 7 | | 135.56.81... | | | | | OK | Not Conta... |
| 8 | | 198.152.2... | | | | | OK | Not Conta... |
| | --- cloud --- reas... | | | | | | | |
| N | | 10.3.0.20 | | | | | Not Pingable | Not Conta... |

| Timestamp | Source | Message |
|-----------|--------|---|
| 11:55:13 | TNode | Node 32.29.23.82 is not SNMP contactable |
| 11:55:13 | TNode | Node 32.29.39.161 is not SNMP contactable |
| 11:55:13 | Path | (router 135.27.66.1/23 10.24.24.2/30) (router 10.24.24.1/30 135.27.81.50/30) (rou |
| 11:55:13 | Path | (router 135.27.66.1/32) (router 10.24.24.1/32) (router 135.27.81.49/32) (router 13! |

When the tool is finished running a dialog will display giving you the option to upload the gathered data so that a report can be generated. Click **OK** to upload.



The Controller is about to upload the dataset to the Avaya FTP server. The FTP parameters seen in this dialog box can be preconfigured from the Controller's configuration menu.

Dataset Name: .pgp

FTP Server Name: ftp.avaya.com

User Name/ID: expertnetlite

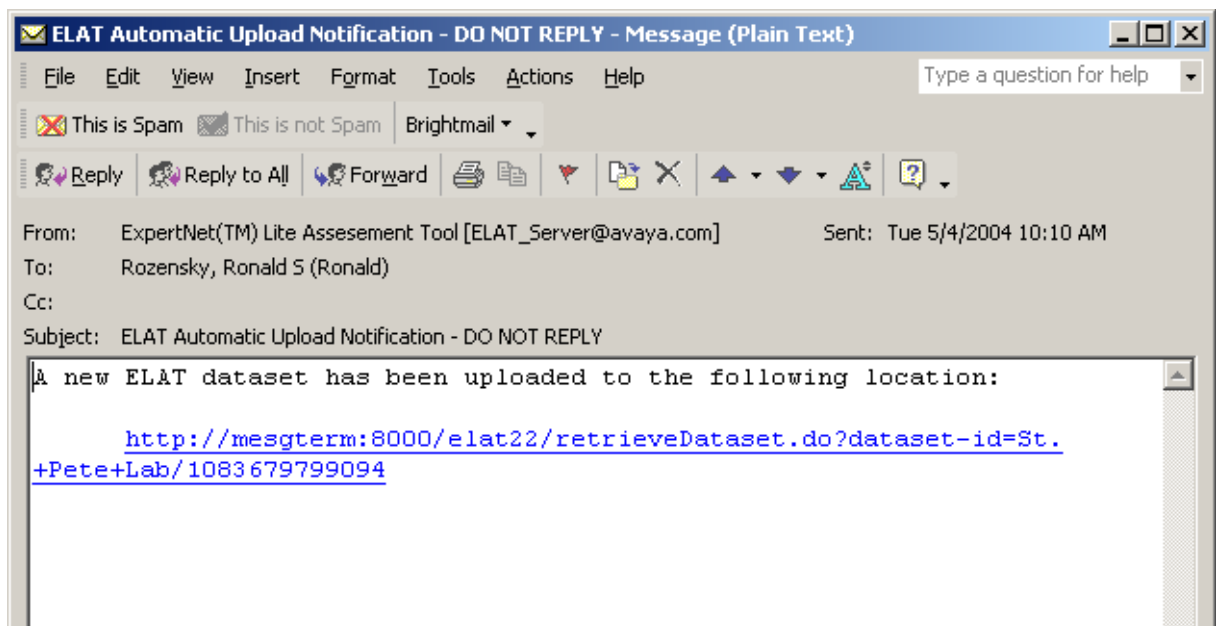
Password: xxxxxxxx

Buttons: OK, Cancel

If the automatic upload fails for any reason, you can use the Upload button to try again, or email the dataset to the ELAT support team (elatsupport@avaya.com).

Automatic Upload Notification

The ELAT server polls the Avaya external ftp server on a regular basis. Once the ELAT server finds the dataset automatically uploaded, you will receive the following email.



Avaya Associates

Avaya Associates should then access the ExpertNet Lite web server and download their report. For further information see [Appendix C: Avaya Associates: Downloading the Report](#).

Avaya BusinessPartners

BusinessPartners will receive an email with encrypted version of their report from their ELAT representative.

When assessments are complete

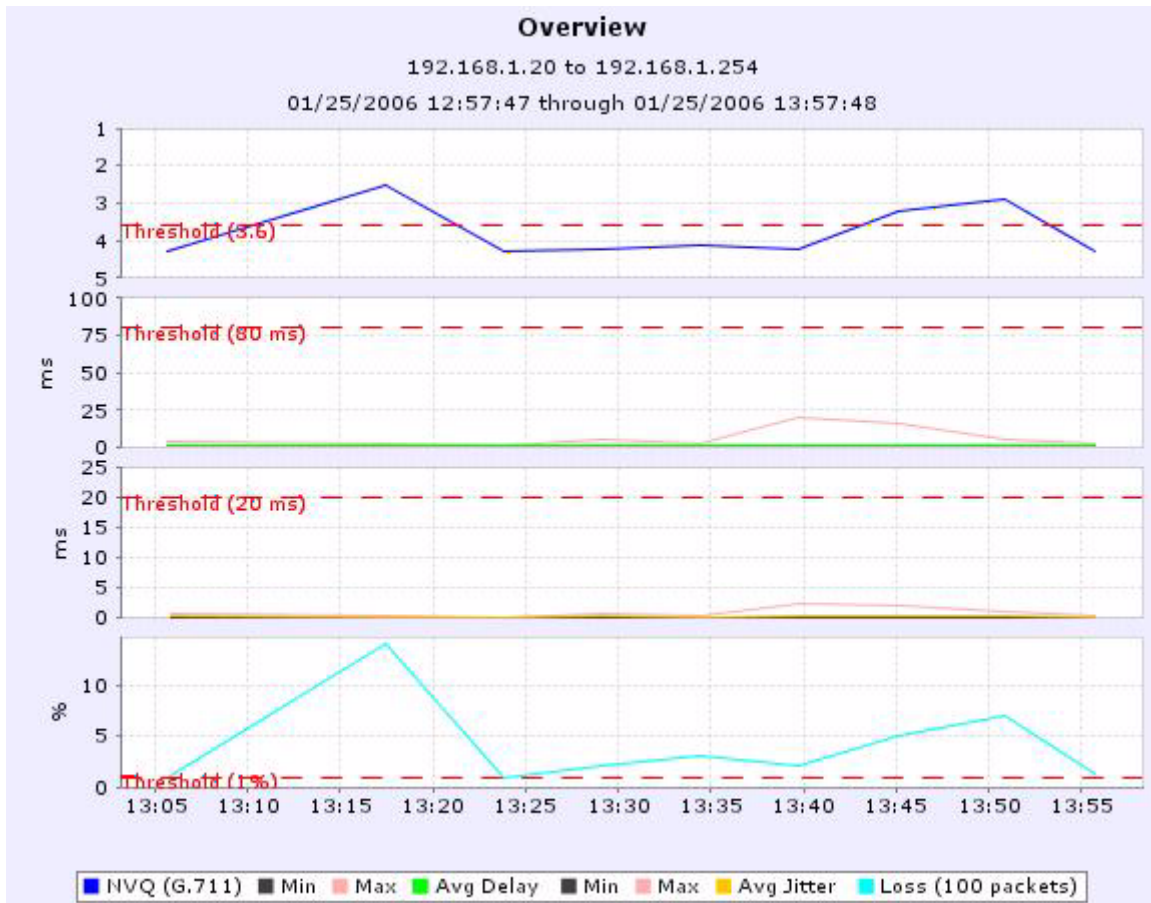
After assessments are done, it is recommended that you remove the Traffic Simulators from the PCs they are installed on.

Analyzing the Report

Reports are generated in RTF format and can be viewed and edited in Microsoft Word. All reports contain the following sections:

- Introduction to Avaya Basic Assessment report
- Executive Summary
- Background on data
- Series of charts
 - Performance summary – entire network
 - Overview – per path or target
 - Delay
 - Jitter
 - Loss
 - Ping Response
 - CPU – if SNMP data gathered
 - Interface – for most devices
- Recommendations and technical information on VoIP

Overview Graphs



- Overview chart is available per path or target
- Delay and Jitter have maximum, average, and minimum values-max and min are only in the overview chart
- Average is over a 10 minute period

QoS Graphs

Separate graphs displaying Delay Jitter and Loss are available for each target.

PATH

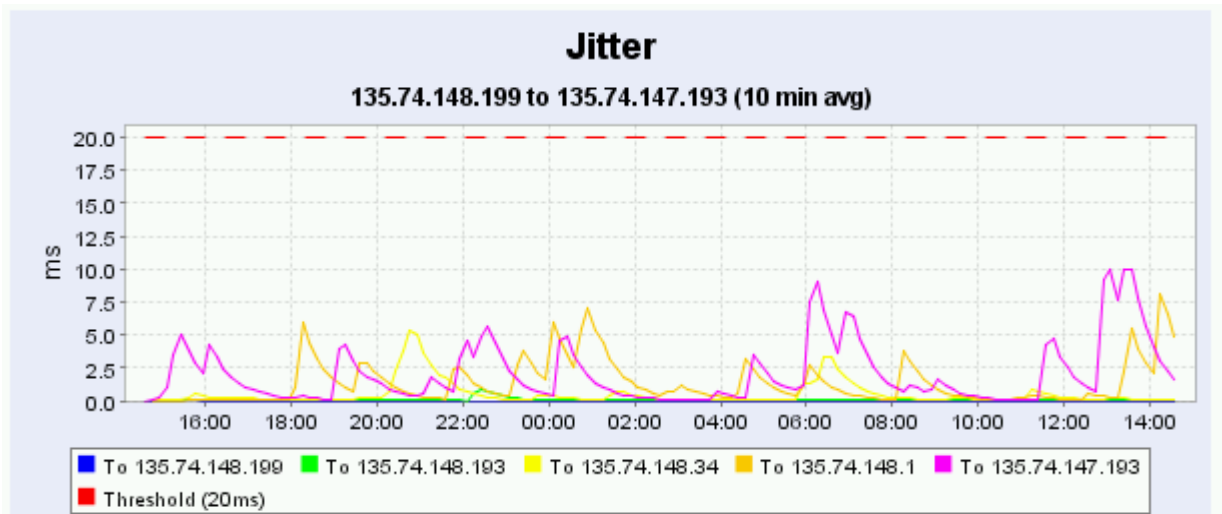
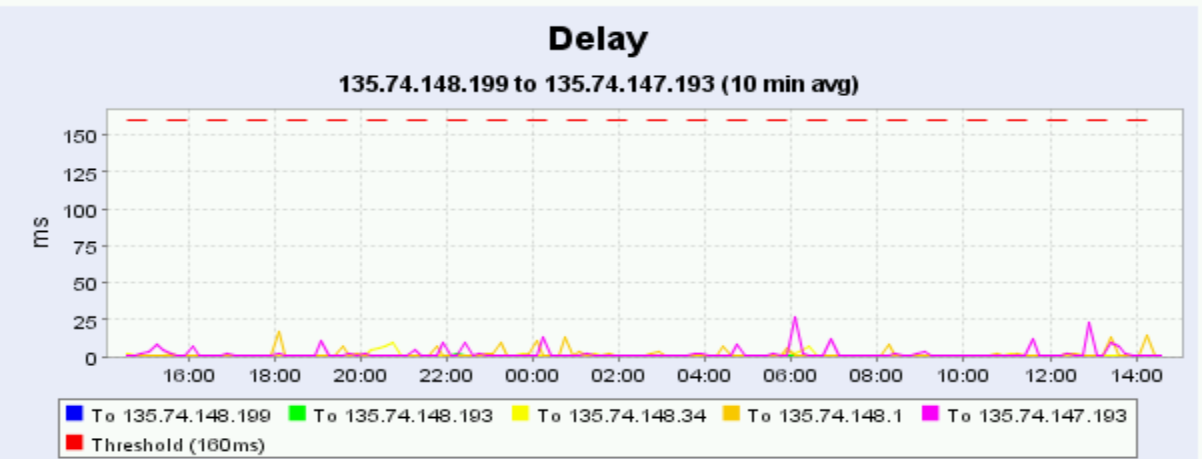
AGENT [135.74.148.199]

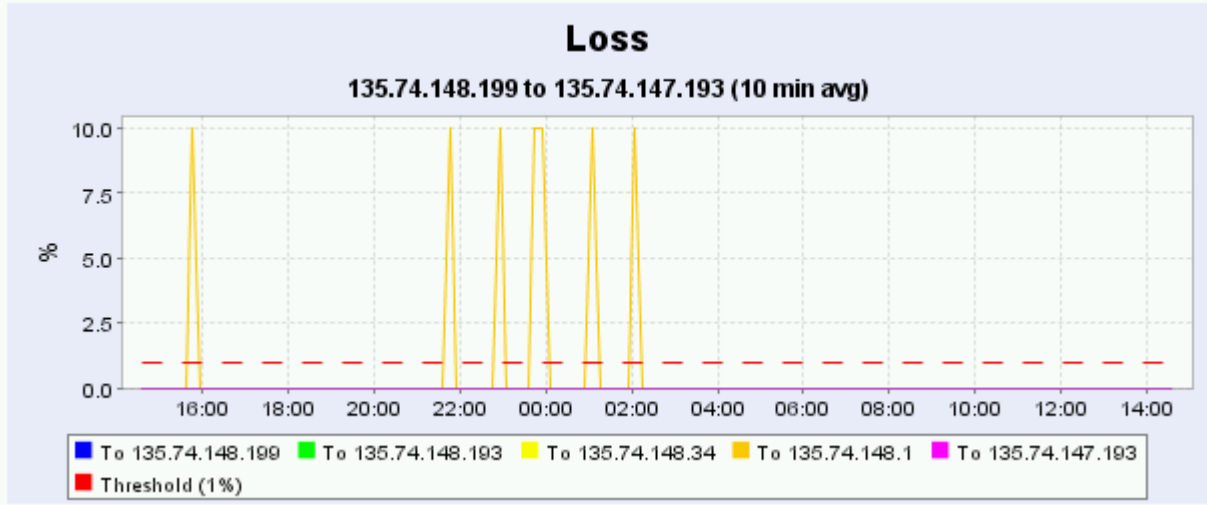
ROUTER [IN: 135.74.148.193 OUT: 135.74.148.33]

ROUTER [IN: 135.74.148.34 OUT: 135.74.148.6]

ROUTER [IN: 135.74.148.1 OUT: 135.74.147.194]

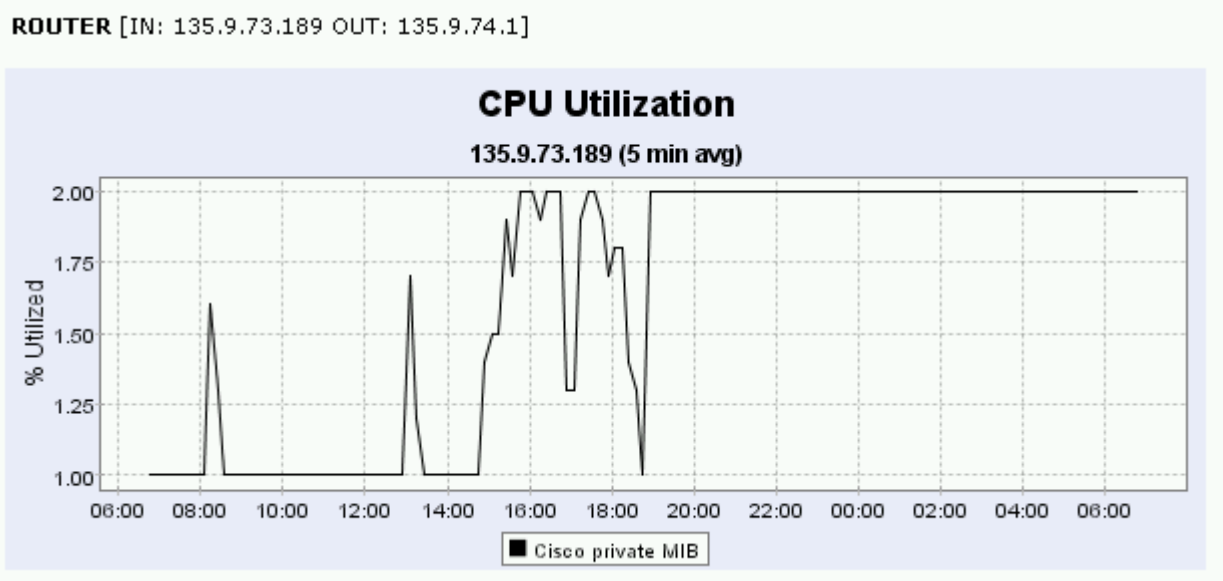
ROUTER [IN: 135.74.147.193 OUT:]



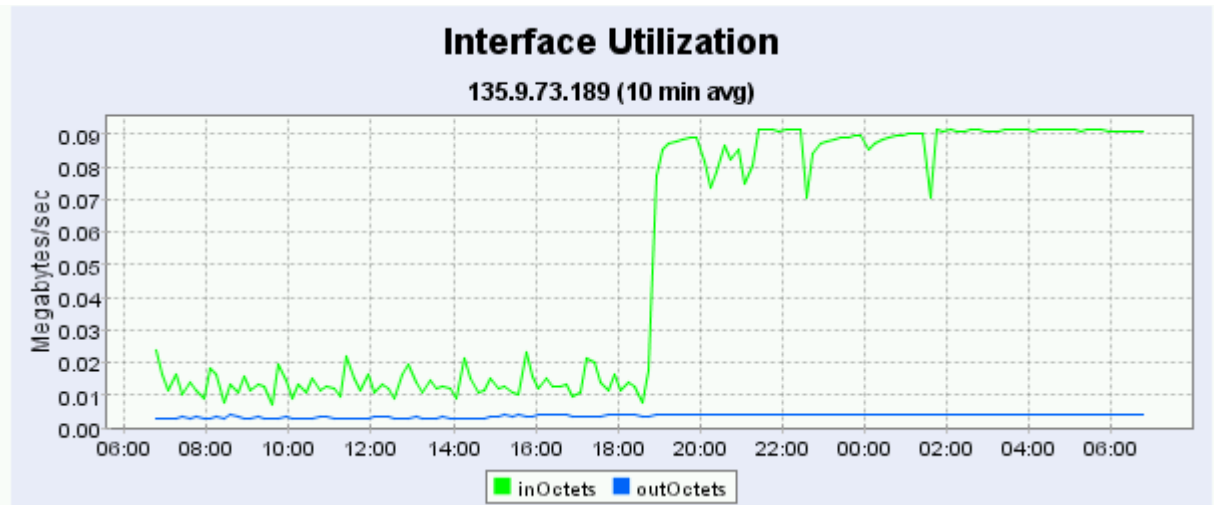


SNMP Data

If SNMP access to routers is enabled, and read community strings are available graphs displaying performance criteria will also be available.¹



1. This feature is only available for Cisco Routers, Cajun, Extreme, 3Com, Xylogics devices at this time.



Troubleshooting

Q: My customer does not want to give us the community string. Is there a workaround to not giving Avaya or its representatives the community string(s)?

A: Without the community strings we cannot retrieve performance criteria (CPU, interface) from devices. A workaround is to ask the customer to create temporary Read community strings that expire or will be deleted when ELAT has concluded data collection. Once the community strings expire or are deleted, the community strings in the dataset will no longer be valid and will not compromise the customer's network. We recommend "public" or "Avaya" as the Read community strings. Please have the customer verify that the community strings will expire after data collection has concluded.

Q: Why do I not see a path that I was expecting to see?

A: The following are some of the reasons why you do not see the expected path:

- The EDT may not discover the desired subnet because, either there is no read SNMP community string available for any of the devices along the path, or the sub-network is out of scope limit.
- The ELAT Controller could not complete the "traceroute" to the desired host.
- The expected path is part of another long path, in which case, the expected path was removed as a Redundant path.

Q: Why do I see 100% packet loss for a given path?

A: The following are some of the reasons:

- Some devices are not responding to UDP ping which will show up as 100% packet loss. Use the udping utility located in the /bin directory to verify that the device does respond to UDP ping.
- The Network might have changed during the data collection phase, in which case, the device is not reachable.

If the device responds to an ICMP, but not a UDP ping, use the ICMP option.

Q: Why are there no interface statistics for one of my routers?

A: Usually this is caused when the device does not support the standard MIB-2 interface counters. This is common for Avaya Cajun devices in particular. Please verify the inOctets / outOctets and inDiscards / outDiscards are available using MIB browser.

Q: Why is there no CPU utilization for one of my routers?

A: There are several reasons why CPU is not being reported:

- CPU is supported for some (not all) devices manufactured by 3Com, Avaya, Cisco, Extreme, and Xylogics.
- Older devices may not support SNMP
- The community string was not provided, or is not correct.

Q: I just created the license file and the customer is receiving a license expired message-why?

A: The license file is a window to run the ELAT Controller - there is a definitive start time (when the license was generated) and end time. The start time is the date and time the license was generated on the ELAT Server. If the customer Windows computer has a date-time before the license was generated, the ELAT Controller will report that the license has expired. There are two ways to solve this problem:

- Change the date and time of the Windows computer.
- Wait until the Windows computer date-time passes the license file generated date-time.

Q: I have multiple routers attached to the Controller PC subnet. Will this work?

A: Yes it will work as long as the default gateway from the Controller PC is reachable and SNMP enabled.

Q: Is there a rule to select the edge devices when run in Target mode?

A: The rule is to select any IP device that responds to the udping utility. However, we have found that Printers and some Sun Servers do not fare well in responding to the UDP pings.

Q: Why is it that when I attempt to upload a dataset I receive an error?

A: There are two possible scenarios:

- The upload is taking longer than the timeout session for the browser. Verify that the browser is bypassing the proxy server for local addresses. Try doing the upload early in the morning or late at night when network traffic is lowest. As a last case, copy the dataset to the field problems server and open a ticket with the STARS team at http://gsomissrv2.global.avaya.com/request_system/request.asp?tools_team=1
- When the dataset was copied from one computer to another it was corrupted. For example, ELAT is run on a Windows XP box. When it is done running, you ftp it to another computer. When you use the ftp command, the binary option was not used, so the file was not transferred in a binary format. When you upload the file to the ELAT server, there is an error. To correct for this problem, always transfer the file in binary format.

Q: Where are the log files stored?

C:/Program Files/Avaya/ELAT/logs

Q: Can I use network devices as endpoints of a path?

A: No, you should avoid using network devices if at all possible as endpoints. There are several reasons why this should be avoided:

- The goal of ELAT is to measure the entire path, from where ELAT is deployed to where an IP phone hypothetically would be located, which include the last network device on the path. If you use that device as the endpoint, you are no longer measuring the devices' delay, loss, and jitter, but the path to it. If the device is saturated on the egress interface(s), you will never know-it's the endpoint and we don't use the egress interface, only the ingress.
- Some network devices will throttle ICMP responses to a UDP port unreachable, but will pass-through the pings. Let's say we have a router and the CPU is at a high utilization and we are using it as the edge host. We do a UDP ping - and the router holds onto it until the utilization drops - and then sends the response. Or the router just ignores the UDP ping entirely. Either way, the results are skewed.

Q: What devices should I use as endpoints?

A: For RTP tests endpoints must be Windows XP boxes with the Avaya Traffic Simulator installed.

For Ping tests, PCs or UNIX workstations are preferred. The hardware is typically very stable, and many PCs or workstations will respond to pings quite efficiently. Network hardware (listed above) should be avoided if at all possible. Newer printers may be used, but ping (UDP and ICMP) them first to ensure that they will respond. If you are using laptops, verify that the laptops will not hibernate or go into standby mode during the engagement.

Q: What ports does ELAT use?

A: ELAT uses a range of ports. The ports range between:

24000 - 26000 and 27000 - 34000 with the exception of port 33711 and 33712.

It also uses the port range 2048 to 3389 for RTP Tests. Note that it only requires the first 100 or so ports in this range to be free.

See: C:/Program Files/Avaya/ELAT/config/config.xml for further details.

Q: How does the SNMP access work? Is it read only? What variables are retrieved?

A: The SNMP access is read-only. The Controller collects processor and interface utilization variables. Processor utilization is supported by proprietary OIDs (cpmCPUTotal5sec and busyPer for Cisco, a3sysCpuUtil for 3Com, extremeCpuAggregateUtilization for Extreme, genCpuAverageUtilization for new Cajun

devices, cpuUtilization for Xylogic). Interface utilization is retrieved from standard MIB2 (ifInOctets, ifOutOctets, ifInDiscard, ifOutDiscards). If ifXTable extension MIB is supported on a device, high-precision values ifHCInOctets and ifHCOutOctets are retrieved instead of ifInOctets and ifOutOctets.

Q: The Delay graphs show a threshold of 80msec. Is this one way or round trip?

A: All measurements are in one way delay. RTP tests can determine one way delay without needing RTT. Ping tests are actually recording RTT and dividing by two.

Q: How long will a dataset remain on the server?

A: Datasets are archived after approximately six months. If this is not convenient, or will interrupt your project, please let the ELAT team know.

Q: ELAT was not run in the network that it should have been. Can I rerun ELAT with the same license file and same customer name?

A: License files are valid for a maximum of 30 days. As long as the license has not expired when ELAT is started it will run.

Q: I need to rerun ELAT with the same customer at the same location. Will the first dataset be overwritten?

A: No. We do not allow or support overwriting datasets. All datasets are considered unique and stored separately, irrespective of how many times ELAT has been run at a customer location.

Q: How much traffic does ELAT create on a network?

A: The ELAT Controller generates very little traffic. Default settings in <ELATControllerBaseDir>\config\config.xml are:

1. Average number of pings/second is 2.
2. Maximum of 2 SNMP get requests/second. This is a default throttling parameter, not an average value. SNMP poll interval for each node is by default equal 60 seconds. It means that if there are 10 SNMP-polled nodes, each of them will be polled every 60 seconds, so there is a SNMP GET request issued to the network every 6 seconds in equal intervals

Ping datagrams are 180 bytes. SNMP PDU's can vary from about 100 bytes to a few kilobytes per request, depending on the amount of information per node. RTP traffic datagrams range in size depending on the payload and can vary between 180 to about 300 bytes.

Q: How much bandwidth does ELAT use?

A: For each simultaneous call in an RTP test ELAT uses the expected bandwidth for a single actual VoIP call.

Q: How does the throttling mechanism work?

A: The throttling mechanism is separate for ping and SNMP polling. For SNMP, configuration wizard in "Step 4: SNMP Settings" exposes Poll Interval of Single Node[secs] and Maximum Total Number of Polls/Sec parameters. Poll interval defines a polling frequency of each node. The second parameter limits the total number of SNMP polls issued to the network. (Maximum Total takes precedence over Poll Interval: if Poll Interval is too small, it is automatically recalculated by the Controller to satisfy the Maximum Total). The default Poll Interval is 60 seconds, Maximum Total is 2.

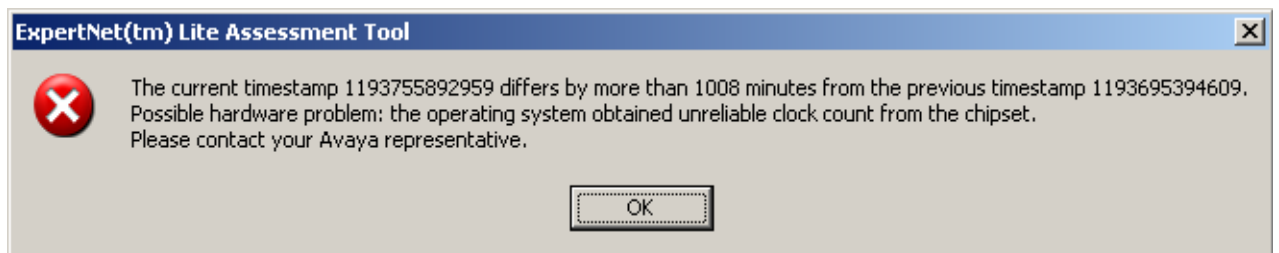
For ping polling, the configuration wizard in "Step 5: Ping Settings" exposes the 'Avg Number of Polls/Sec' parameter which determines the frequency of sending pings to the network. The default value is 2.

Q: There is a Diffserv value in the config.xml file. Does that tag UDP packets? Is this one direction or both?

A: The ELAT Controller has the ability to tag UDP packets as diffserv. These packets are outbound only; the response is an ICMP port unreachable, and is not tagged.

Q: Our report shows that the network fails the analysis, but there isn't much loss and delay and jitter look acceptable. Why the failure?

A: Check to see if there is IPX or raw Netbios (not IP encapsulated) on the network. These protocols do not respond to IP QOS and will not show up as IP traffic, but will affect the IP traffic.

Q: I get the following error message on start up.

S

This is a known bug that occasionally happens on certain machines. It should only occur once and then you should be able to continue.

Q: Upon start up, ELAT presents an error dialog showing: "Route redirection is not disabled on this machine..." and then shuts down.

A: Typically the installer will set this registry variable on the controller PC. Occasionally this will not work and it will have to be set manually.

- Open the registry with START -> RUN -> 'regedit'.

- Navigate to
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
EnableICMPRedirect and then set the value of this parameter to 0.

Q: The Traffic Simulator is on a machine with dynamic IPs and its IP keeps changing.

A: The ELAT Controller identifies the Traffic Simulator by IP address and not MAC. If the IP address does change, then the old entry for the Traffic Simulator needs to be removed and the Traffic Simulator would need to re-register.

Q: Imported paths fail to run properly during a measurement run.

A: Whenever paths are imported, it is important to do a verification test to ensure that the RTP Traffic Simulators that are indicated are actually registered with this ELAT Controller and hence can be contacted for doing the test. If the Traffic Simulators do not respond to the ELAT Controller, they will have to be restarted.

Q: RTP tests fail when used on a machine with an active VPN connection.

A: ELAT cannot run RTP tests if the controller or traffic simulator in question is on a device with a VPN driver as this causes conflicts with the driver used by ELAT.

Appendix A: Installing the Controller and Test Agents

Installing the ExpertNet™ Lite Assessment Tool Controller

1. Double-click on the installer icon
2. Click Next.
3. The license agreement is presented. Accept the agreement and click Next.
4. Keep the default values and click Next to install all features to the default location.
As well as the ELAT Controller, this will install the ELAT Web server. This is a lightweight application that is only active for the period the ELAT controller is active. It will enable to to install the Avaya Traffic Simulators more quickly and easily.
5. You are now ready to install the application, click Next.
6. Click Finish to complete the installation.
7. Now you are presented with the Reboot window. Click Yes to reboot the PC.
8. You are now ready to install the license key. You should have received the license key from Avaya (usually via email). It is a file named "license.txt". Paste the file into the ELAT config directory. If you installed the device to the default location the path is C:\Program Files\Avaya\ELAT\config directory. If there is an existing file with the same name replace it.
9. For information on running ELAT, see the "ExpertNet Lite™ Assessment Tool User Guide, Version 3.0".

Installing the Avaya Traffic Simulator™

The Avaya Traffic Simulator has to be installed on remote endpoints in a customer network. The easiest way to get the application onto customer machines is to download via the web server onboard the ELAT server.

If you did not select the option to install the Web Server when installing the Controller you can download the Traffic Simulator from the support.avaya.com portal.

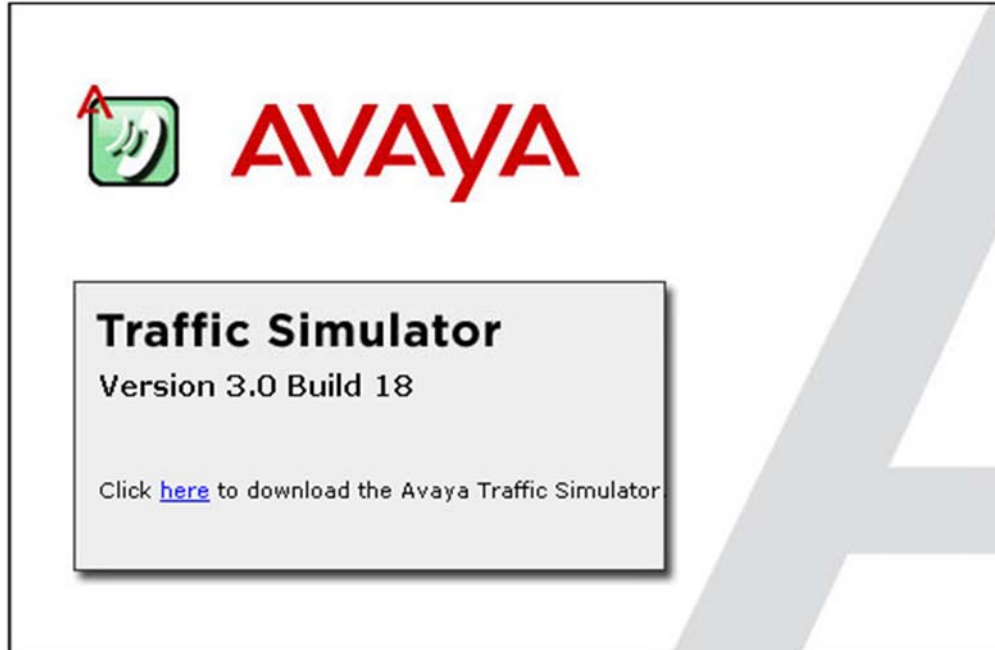
Note: A Traffic Simulator will be installed on the ELAT controller PC by default on an ELAT installation. This Traffic Simulator can only be uninstalled by uninstalling ELAT. The remote Traffic Simulators can be uninstalled at any time.

1. Launch the ELAT Controller.
2. On the remote Traffic Simulator PCs, open up a browser window. In the Address field, enter the IP address of the ELAT controller PC. If you have changed the Web

Server port from the default value of 80 you need to navigate to `http://<controller_ip_address>:<port_number>`

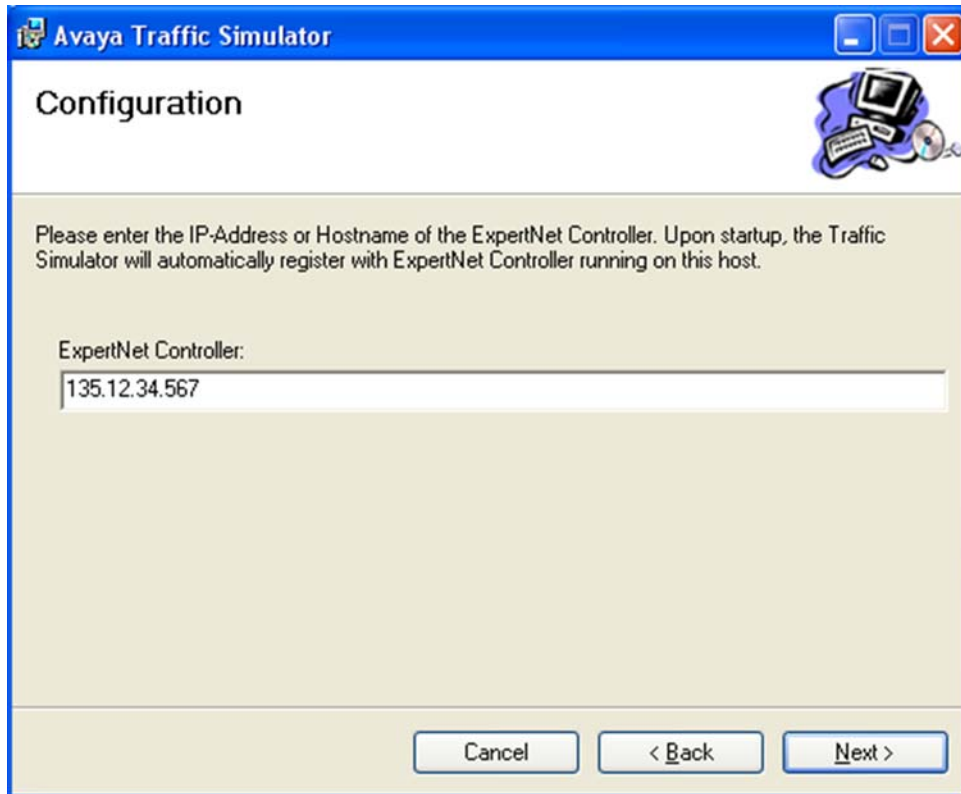
NOTE: To find the IP address of the PC open the **Control Panel > Network Connections > LAN Area Connection** dialog and open the **Support** tab.

3. On the page that displays, click the link to download the test agent.



4. On the dialog that displays, click **Run**.
5. On the first screen you can see what version of the Traffic Simulator you are running. Click **Next** to continue.

6. On this page enter the IP Address or hostname of the Controller and click Next.



7. Enter the install location, use the default install location and click Next.
8. You are now ready to begin the installation. Click Next.
9. Click Close. The machine's network connection will be momentarily disrupted. This disruption will typically take 30 seconds at most.
10. A window displays giving you the option to reboot now or later. Click Yes to reboot the PC. Rebooting is required to collect DSCP data. Upon start-up the Traffic Simulator will contact the ELAT controller. The Traffic Simulator Monitor icon is now available on the system tray for additional configuration if required.

Appendix B: Firewall Configuration

If you have installed Avaya ExpertNet Lite Assessment Tool or Avaya Traffic Simulator on a computer with a firewall installed, you may find that RTP tests fail. This may be due to the test data being discarded by the firewall. You may configure common firewalls to allow Avaya ExpertNet Lite Assessment Tool or Avaya Traffic Simulator to be exempt from the firewall's usual rules.

To configure Windows Firewall:

1. Open the Windows Firewall Configuration (Control Panel, Windows Firewall)
2. Click the **Add Program** button found on the **Exceptions** tab.
3. Click **Browse**, and select **C:\Program Files\Avaya\Traffic Simulator\TrafficSimulator.exe**
4. Click **OK**.
5. Ensure the **Don't allow exceptions** tick box is un-checked in the General tab.

To configure McAfee Personal Firewall:

1. Open McAfee Personal Firewall.
2. Select **Personal Firewall Plus** along the left side.
3. Click **View** the Internet Application List.
4. Find **Traffic Simulator** in the Application Name column.
5. Right-click **Traffic Simulator** and select **Allow Full Access** (If you don't see Traffic Simulator in the Application Name column, click **Allow New Application** and enter **C:\Program Files\Avaya\Traffic Simulator\TrafficSimulator.exe**)
6. Exit McAfee Personal Firewall.

To configure Norton Personal Firewall:

1. Open Norton Personal Firewall.
2. Select Status & Settings from the left menu bar.
3. Choose Personal Firewall from the middle column.
4. Click Configure.
5. In the new window, open the Programs tab.
6. Find Traffic Simulator in the Manual Program Control table.
7. Click the Internet Access column for Traffic Simulator, and select Allow All.
8. Click OK.

To configure PC-Cillin Internet Security:

1. Open PC-Cillin Internet Security
2. Click **Network Security** along the left side.
3. Click **Edit**.
4. From the **Personal Firewall Profile** window, open the **Exception List**.
5. Click **Add**.
6. Enter the following information in the appropriate fields:
 - Description: Avaya Traffic Simulator
 - Target: Specified Application (enter **C:\Program Files\Avaya\Traffic Simulator\trafficSimulator.exe**)
 - Action: Allow
 - Ports: All ports.
7. Click **Save**.

To configure Tiny Personal Firewall:

1. Open Tiny Personal Firewall.
2. Go to the **Administrator Center**.
3. From the **Groups** menu, click **Trusted**.
4. Click **Enroll**.
5. Enter **Traffic Simulator** in the application name field, then enter **C:\Program Files\Avaya\Traffic Simulator\TrafficSimulator.exe**
6. Click **Save**.

To configure ZoneAlarm:

1. Open ZoneAlarm
2. Select **Program Control** along the left side.
3. Find **Traffic Simulator**, and click each red **X** so they are now green.
4. Select **Allow**.
5. Exit ZoneAlarm.

Appendix C: Avaya Associates: Downloading the Report

Download Report

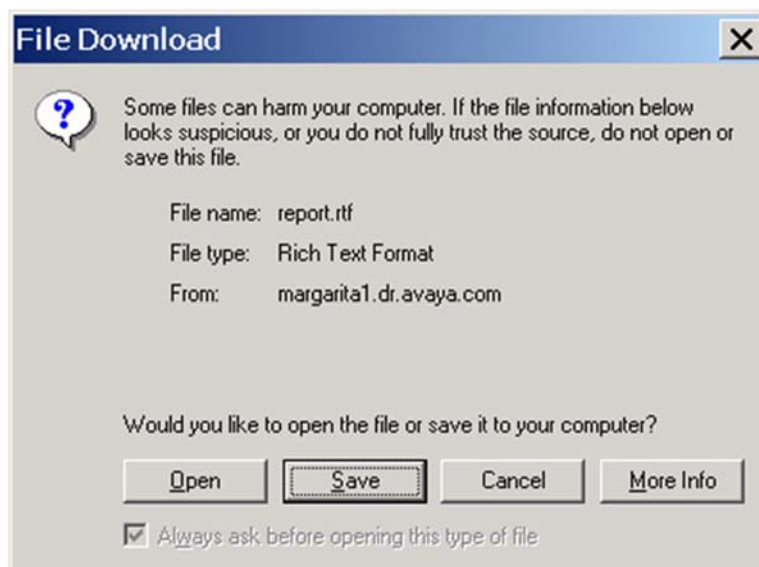
Once the dataset is uploaded, you will be able to view and analyze the data by generating a report.

1. Click on ExpertNet™ Lite Home link. Then click the View Datasets link.
2. Click on Download for the appropriate Customer ID. ELAT partitions datasets to allow you to view only datasets uploaded by you and other members in the group. The current User ID and the group name that he belongs to, is displayed on the web page. If the User belongs to multiple groups, all groups are listed.

The ELAT server has functionality to generate a Rich Text Format (RTF) report with charts. In the default functionality, all paths or targets are selected for inclusion in the report.

As of ELAT 3.0, reports have been modified to support a new format. Paths may be described twice if they were given different characteristics, (for example, different DSCP level, different codec and so on).

The server will process your request, and depending on the size of the dataset and the number of elements may take several minutes. Once processing is complete, you will be prompted with the following menu.

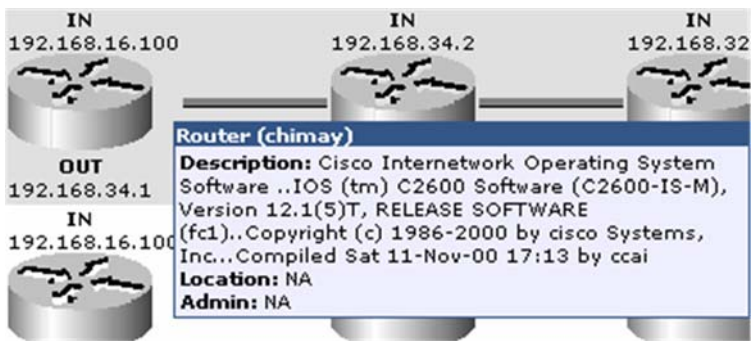


You may open the file, or save for later use. The report is dynamically generated from a RTF template and an XML data source, so there is no chance of acquiring a virus or worm from the report.

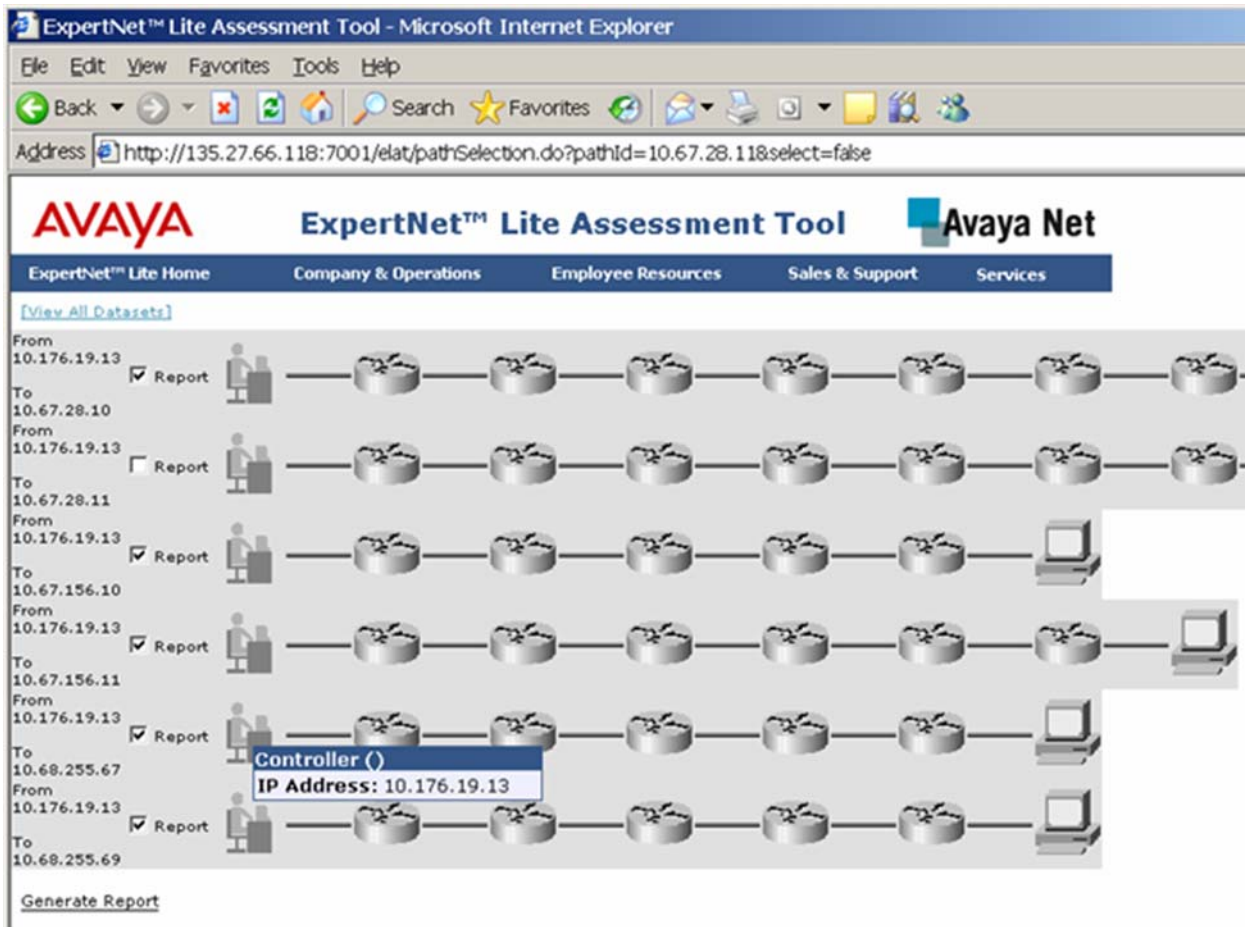
Generate and Download Custom Reports

A custom report that excludes certain targets or paths can also be generated.

1. Select the Generate link in the Custom Report column on the View Datasets page.
2. You will be presented with a graphical representation of the paths.
3. Select or deselect the checkboxes next to path, as shown in the following image.
4. You can get information by hovering the mouse over the object:



5. To generate the RTF report, select the Generate Report link.



Glossary

| | |
|--|---|
| ExpertNet™ Lite Assessment Tool | A tool designed to assess whether a customer network is ready to support VoIP calls |
| ExpertNet™ Discovery Tool | Internet Protocol discovery, visualization, analysis and display tool, bundled with the ExpertNet™ Lite Assessment Tool and not supported as a standalone tool |
| ExpertNet™ VoIP Assessment Tool | A more sophisticated Avaya tool for determining whether a customer network is ready to support VoIP calls. It, for example, can simulate higher call volumes than the ExpertNet™ Lite Assessment Tool |
| ICMP | Internet Control Message Protocol |
| IP | Internet Protocol |
| MIBs | Management Information Bases |
| OSPF | Open Shortest Path First (routing protocol) |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| RTP | Real-Time Transport Protocol |
| RTT | Round-trip time |
| SNMP | Simple Network Management Protocol |
| TCP | Transmission Control Protocol |
| TTL | Time-to-live |
| UDP | User Datagram Protocol |
| VoIP | Voice over Internet Protocol |
| NVQ | Network Voice Quality - an estimate of the Mean Opinion Score of a call using packet-level measurements |

End of Document
